Foreword

Society is getting to be more and more dependent on the reliability of the Internet. Businesses are relying on the Internet as their link to their customers. Customers are being encouraged to do most of their business in the Internet.

It is not enough to protect your communication from eavesdroppers, or to protect your own system from being infected with viruses. Traditionally, the security community has focused its attention on unauthorized disclosure or modification of information, and perhaps theft of services. Denial of service was largely ignored as being unlikely to occur because the attacker would not gain anything from such an attack.

Clearly this is not the case today. Denial of service can be a devastating attack. It can put merchants out of business and can cause major and very visible disruption to our world. It can be (and is) used against specific companies for which the attacker has a grudge or has been paid to attack; or it can be used by terrorists to cause major disruption to critical infrastructure.

As widely publicized denial-of-service attacks occur, the subject is finally getting needed attention. Not so long ago, it was assumed that the amount of damage any attacker could do was limited by the speed of that attacker's Internet connection. If that were true, it wouldn't be too hard to find the attacker's machine, filter out its packets, disconnect it from the Internet, and prosecute the machine's owner (presumably the attacker). Unfortunately, attacks grew more sophisticated. Instead of attacking directly from the attacker's own machine, an attacker breaks into a lot of machines, and causes them to attack. The attacks are now coming from many machines owned by innocent, if careless, owners.

Why is it so easy to break into machines? Unfortunately, there is little incentive for vendors to provide secure software, and little incentive for owners of machines to keep up with patches and turn security on in their machine. Vendors are in business to make money. Time to market, fancy features (which are likely to introduce vulnerabilities), and price are more important differentiators than security. A vendor that provides a low-frills product that goes to market later due to stringent testing will lose in the marketplace. If manufacturers were routinely sued for security bugs in their products, perhaps security would feature more prominently in the economic equation.

It is tempting to blame the users. Why don't they install patches promptly? Why don't they turn off dangerous features such as cookies? However, it is completely unfair to blame the users. Users are getting less and less sophisticated. When computers were used primarily by university computer science students, it was reasonable to make them arcanely difficult to manage. Today just about everyone is using computers, and is expected to manage their own systems. And when there are features that can be exploited by attackers (such as ActiveX), users can't simply turn these features off, because many Web sites wind up using these features. Not because they need to, but because the features are there. If users say no to anything, they get strange error messages and all sorts of things stop working.

Fighting denial of service is going to be a constant spy vs. spy game. The good guys (the defenders) will try to defend against all the known attacks, and the bad guys (the attackers) will try to disguise their attacks to stay under the radar. It is good that the good guys have been awakened to the need to be ever vigilant, and to get ahead of the game through research.

This book is timely and written by an ideal author team. It is crucial to understand the world as currently deployed, and it is also crucial to look to the future. This author team provides expertise along the whole range. David Dittrich, of the University of Washington's Information School and the Center for Information Assurance and Cybersecurity, is one of the foremost frontline DDoS fighters today, and indeed, an "I'm feeling lucky" Google search for DDoS brings up the DDoS page that he maintains.

Jelena Mirkovic did her Ph.D. work at UCLA, with advisor Peter Reiher, on innovative approaches to DDoS defense. Their work produced the first source-end DDoS defense system, which helps network administrators ensure that poorly secured machines in their network cannot be misused to attack others. They also worked on developing taxonomies of DDoS attacks and defenses, and defining methods for measuring the success of defenses. Jelena continues her fight against DDoS as an assistant professor at the University of Delaware.

Sven Dietrich is a researcher at the CERT Coordination Center. He is part of the research group that investigates the survivability of networked systems. The CERT Coordination Center is the first organization of its kind, and has helped to start similar organizations around the world. It is likely to be the first place to hear about attacks, and to marshal the resources necessary to provide defenses. Sven also works closely with Carnegie Mellon CyLab—a cybersecurity research and education center. Following their meeting at the CERT DSIT Workshop, Sven teamed up with David Dittrich and others in producing analyses of several early DDoS tools.

—Radia Perlman