When the Internet’s precursors began — as research projects in the US government and academia — they were small, cooperative networks that looked toward a broader goal of a robust, worldwide network in which the constituent parts worked together for the benefit of the whole. One university might send its data packets through another to get them to a third. Domains would be offline for significant periods. Servers would use dial-up modems to connect briefly to see if there was any work for them to process.

Everyone was happy to relay each other’s packets, and everyone “played nice.” If a computer system did something untoward, improper, or damaging, it was usually due to faulty software, misconfiguration, or prank-playing. In any case, it was easy to track down the cause or the culprit and sort it out — and no one wanted their network nodes to be disconnected, banned for bad behavior.

Because of this background, network protocols, from the lower layers up to the application layer, were designed with fairly little protection. Consequently, spoofing of everything from IP addresses to email addresses is now possible. Packets can be inserted to fool name resolution (Domain Name System) requests. Passwords can be intercepted en route. Excessive data volume can overwhelm a server or an entire network. Many protocols started life with no authentication mechanisms in them and lacked any provisions for checking the legitimacy of either side of the transaction.

Of course, there was also little incentive to violate the spirit of cooperation. The early Internet wasn’t used for commercial purposes: “dot com” used to refer to the research and development arms of commercial companies, not to their marketing and sales departments, and actually buying and selling things online was hardly practical.

Then, as one wag has put it, “The
Guest Editor's Introduction

world changed profoundly and unpredictably the day Tim Berners-Lee got bitten by a radioactive spider.” Berners-Lee wouldn’t liken himself to a superhero, but his vision of the Internet as an interconnected Web of data, a vision that took FTP and Gopher and turned them on their heads, has enabled an explosion of activity and usage beyond what anyone imagined. Grandma is now on the Internet.

The Modern Internet

Now, there are plenty of reasons not to play nice. There’s business to be hawked, money to be made, information to be gathered — legitimately and ethically, or otherwise. There are incentives to send unsolicited messages, incentives to surreptitiously reroute traffic, incentives to take down competitors or detractors, and incentives to hide one’s tracks and evade detection.

Unwanted, unsolicited email — “spam,” colloquially — is the most obvious form of unwanted traffic, and perhaps the only form most Internet users are aware of. Look a little further, though, and we can see spam in the form of instant messages, blog comments and trackbacks, and Internet voice messages. We see junk blogs, phony social networking accounts, and entire bogus Web sites. “Link farms,” “click spam,” and phishing are all forms of unwanted Web traffic. “Search engine optimization” (SEO) — the practice of manipulating things so you or your client show up at the top of the search results — is a business of its own, and not always an entirely above-board one. And lower network layers are subject to unwanted traffic as well, as malefactors try to subvert every part of the Internet.

Denial-of-service (DoS) attacks — attempts to overload online services by requesting large amounts of unproductive work — have been in the news quite a lot recently. Over the past year, the New York Times has described DoS attacks in general (www.nytimes.com/2008/11/10/technology/internet/10attacks.html), and we’ve seen coverage of specific attacks on Kyrgyzstan (www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access), sites in South Korea and the US (www.nytimes.com/2009/07/10/technology/10cyber.html), and Twitter’s social messaging service (www.nytimes.com/2009/08/07/technology/internet/07twitter.html).

These attacks are themselves enabled by one result of other types of unwanted traffic: the formation of botnets, or “zombie networks” — underground networks of usurped computers, taken over against the will and without the knowledge of their owners and given orders by controllers on the Internet. In early 2007, Vint Cerf estimated that perhaps a quarter of all computers on the Internet might belong to botnets, and the numbers have only grown since then, as worms such as Storm and Conficker have spread. Conficker alone is thought to have infected as many as 15 million computers (www.upi.com/Top_News/2009/01/26/Virus-strikes-15-million-PCs/UPI-19421232924206/).

DoS attacks mounted by botnets are particularly challenging because of the difficulty in determining the sources’ legitimacy. A normal, everyday Twitter user today could have his or her computer’s hidden zombie mode switched on tomorrow, making it part of the attack. Defenders must expend valuable resources trying to serve that computer until heuristics can determine that it’s part of the attack. Even then, the resulting blacklisting leaves a legitimate user — one who wasn’t even aware of having a role in the attack — without access after the attack is over.

The Challenges

The challenges, of course, are to detect the unwanted traffic without confusing it with the legitimate stuff, to block such traffic without interfering with the real payload, and to add security — authentication, authorization, accountability, integrity, and privacy — without making the whole thing unusable and moving us back to the pre-Web world. Improvements are needed on the common, reputation-based mechanisms of whitelisting, blacklisting, and greylisting.

Whitelisting is the practice of identifying
traffic sources that are known to be good and allowing them to bypass further checking. It reduces delays for such traffic and avoids the possibility that further analysis will misidentify the traffic as bad (false positive). The other side of the same coin, blacklisting, is the practice of identifying traffic sources that are known to be bad and discarding or otherwise disposing of their traffic immediately. This avoids expending resources on further analysis of traffic that we can identify as unwanted very early, and very cheaply.

Greylisting is a technique that plays a trick on the malefactors: suspicious traffic, or traffic from an unknown source, is given a temporary error, depending on the protocol involved. Basically, the source is told that it needs to retry, perhaps after some delay. The hope — and, in many cases, the current experience — is that bad actors often don’t use robust software, the retry will never happen, and the unwanted traffic will have been averted. Good actors, on the other hand, use software designed to deal with these sorts of situations, and the traffic will be accepted on the second attempt.

Beyond these “early warning” mechanisms lie a number of more sophisticated, more resource-intensive, and more error-prone ways to detect and deal with unwanted traffic. Rate limiting, detailed traffic analysis, data analysis (such as deep-packet inspection and content-based spam filtering), and other techniques are used with more or less success. And we’re always searching for better ways.

In this Issue

The three articles presented in this “Unwanted Traffic” issue look at the problems and challenges from different viewpoints.

In “Addressing Unwanted Traffic on the Internet: A Community Response,” Mat Ford and Leslie Daigle look from the viewpoint of the IETF, the organization responsible for many of the standard protocols used on the Internet. A few years ago, the Internet Architecture Board held a workshop in which invited participants analyzed various aspects of the unwanted traffic problem. Ford and Daigle start with the results of that workshop and discuss the underlying factors that contribute to the problem. They consider what can be done — and what is being done — in research, development, deployment, education, and law and policy to fix it.

The authors discuss the money to be made through shady dealings on the Internet and how to restore balance by making malfeasance more expensive. Research on unwanted traffic detection; deployment of DNS Security Extensions (DNSSEC), Domain Keys Identified Mail (DKIM), and other security mechanisms; the education of and collaboration among network operators; and caution in regulation — getting it right and avoiding unintended consequences and loopholes — are key points here.

“DoS Attacks on Real-Time Media through Indirect Contention-in-Hosts,” by Jayaraj Poroor and Bharat Jayaraman, describes a system the authors call operation-trace analysis, which they use to analyze certain DoS attacks on streaming-media services such as Internet television. Such real-time services are more susceptible to DoS attacks simply because of their real-time nature: delays in delivering the data cause more severe effects on user experience than similar delays do with other types of services.

Poroor and Jayaraman look particularly at attacks aimed at other services in the host, which might cause resource contention that slows down real-time services. In these cases, an attack that affects one service appears to be mounted against another — and it needs to cause only enough contention to break the quality of service required to keep the real-time stream running smoothly. The authors show how they put together information about the sequence of operations performed in the host’s protocol stack, and create operation-trace metrics. By analyzing these metrics, they can detect unwanted traffic and suggest ways to mitigate attacks.

Finally, in “Demystifying Cluster-Based Fault-Tolerant Firewalls,” Pablo Neira Ayuso, Rafael M. Gasca, and Laurent Lefèvre consider the use of firewalls to block unwanted traffic. They discuss how firewalls are employed for this purpose, how effective they are, and what performance issues they introduce.

Because firewalls represent a new, and often single, point of failure, their reliability is critical. And because all network traffic is filtered through the firewalls, they can have a significant effect on network throughput. The authors look at fault-tolerant, cluster-based firewalls for these reasons. They describe a variety of firewall configuration options, load balancing
techniques, stateless versus stateful firewalls, and state maintenance/replication issues. Their performance evaluation of the different options advises us of the trade-offs involved in choosing firewall configurations.

The several articles we couldn’t select for this issue due to space limitations represented research and operational studies on other types of unwanted traffic, covering issues such as email, file sharing, and malicious Web content. These projects, and others like them, keep network operators one step ahead of bad actors. Waves of spam and phishing, DoS attacks, malicious Web sites, and the like continue to increase over time. If we can defend against 95 percent of them today, we will need to do better — 98 percent, 99 percent, or more — tomorrow, just to keep the raw numbers manageable.

Because most of the Internet works most of the time, because unwanted traffic is at a point where it’s no more than an annoyance to most people, it’s easy to think that the problem is solved. It is far from solved; continued research and improvement in detection and mitigation techniques are critical to the security and integrity of the Internet.

Acknowledgments

Many thanks to my coeditor, Oliver Spatscheck, of AT&T Research, for his work with me on this issue. Oliver and I would like to express our gratitude to the authors of all submitted articles and to the reviewers for their help in the difficult selection process. We also thank Fred Douglass, IC’s editor in chief, Michael Rabinovich, associate editor in chief, and the production staff at the IEEE Computer Society. Their hard work made this issue possible.

Barry Leiba is an independent Internet standards consultant. His research interests include email and related technology; antispam work, messaging, and collaboration on mobile platforms; security and privacy of Internet applications; and Internet standards development and deployment. Leiba chairs the DKIM and VWRAP working groups in the IETF and the 2010 Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference, and is the editor for the Standards column in IC. Contact him at barryleiba@computer.org.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.