



## BLANKET SECURITY

**Robert Filman** • NASA Ames Research Center, Caelum Research Corp.  
filman@computer.org

It's getting near the holidays, so the Spider turned to see who besides Santa might be breaking in.

### Internet Auditing Project • Liraz Siri •

[http://www.securityfocus.com/templates/forum\\_message.html?forum=2&head=32&id=32](http://www.securityfocus.com/templates/forum_message.html?forum=2&head=32&id=32)

Siri and friends perform a security audit of the "entire" Internet—or at least the first 36 million hosts they could find. They discuss how to find all the hosts (including a top-down recursive download of DNS, scanning the "in-addr.arpa.domain" [see <http://www.isc.org/ds/new-survey.html> for an explanation], scavenging the Network Information Centers for precompiled data files, or buying the information—\$2,500 at the Internet Software Consortium). Having selected one's targets, the limiting resource is not CPU cycles, but network bandwidth.

They estimate that one workstation with a lot of memory and a T3 line could probe the entire Internet in under a week (doing 4,500 "jobs" per minute), while 10 PCs with dial-up connections would take about a month.

As it was, their project used five workstations and took three weeks. They found three-quarters of a million hosts with any of 18 different common security holes. Siri opines

he's far more worried about what a determined hacker could do to the Internet than any old Y2K bug. (Guess we'll have to wait until the eight maids come a-milking to see if he's right.)

The paper is on a SecurityFocus.com discussion forum. SecurityFocus.com describes itself as trying to "facilitate discussion on security-related topics, create security awareness, and provide the Internet's largest and most comprehensive database of security knowledge and resources to the public." In addition to a few papers and the discussion bulletin boards, SecurityFocus also maintains a database of known security weaknesses.

Evidently, poking at other people's computers can invite retaliation, though not quite as much as the author expected. One of the more amusing notes was how the network auditors were themselves hacked by a skillful attacker. Overall, a good read.



### AntiVirus Online • IBM •

<http://www.av.ibm.com/>  
All things about security are not doom and gloom. This IBM site has a collection of readable papers on viruses, memes, and the epidemiology of communicable computer diseases that make things seem not quite as bad as the newspaper headlines. The papers are a bit dated, though, speaking primarily of DOS viruses. The hoaxes

are, of course, fascinating reading, and, as Craig Shergold can assure you, never really go out of style. (The site has little to say about Mac viruses, presumably because (a) it's IBM, and (b) hey, even the virus writers have stopped supporting the Mac.)

Hopeful signs, so to speak, are that more virulent strains tend to get noticed quickly and thus snuffed before they reproduce, and that many of the attacks you hear about are urban legends or hoaxes (which is of small consolation if you really do get slammed by a virus). There are several good papers that plot the incidence of viruses over time and a bit of sociology on virus writers. The site also includes the Wildlist, a catalog of hostile programs assembled by "virus information professionals," and actually encountered on users' machines.

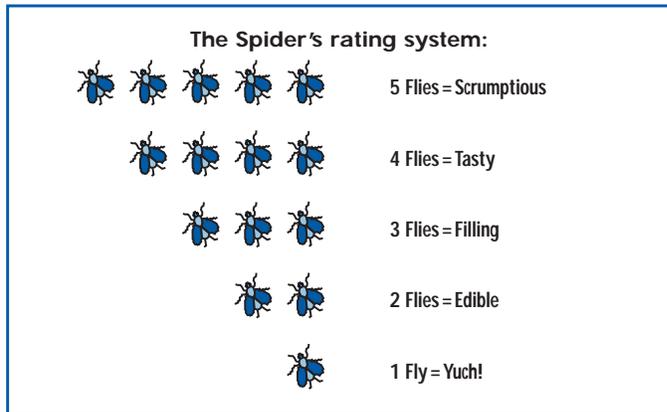
In any case, the antivirus software companies are quick to respond to reports of new viruses. (I wonder if the business plans of any antivirus software companies include writing viruses? Seems like a good way to ensure demand for your product, not to mention bragging rights for being the first to find the appropriate immunization. Sort of the tobacco model applied to personal computing.)



### Onion Routing • Naval Research Laboratory •

<http://onion-router.nrl.navy.mil/>  
I've heard it said that the manager of the Domino's Pizza near the Pentagon is among the first to know when a military operation is in the works (lots of people working late and ordering pizza). Even if you can't read the communication between two sites, there's a fair amount of information in traffic analysis.

Want to hide the pattern of your communication? Follow the lead of The Cardinal in the Kremlin, and pass the message through many intermediaries. The Internet realization of this idea is the Naval Research Lab's Onion Router. Encrypt a communication and mail it, and spies can still read the envelope. Encrypt the communication and the envelope, put that in an envelope addressed to an intermedi-



ary, encrypt that envelope and communication and put it in an envelope addressed to yet another intermediary, and so forth. Send the message to the last intermediary. At each stop, the intermediary extracts the envelope in its envelope and forwards it. Since everything is encrypted, lots of messages are being forwarded at once, and the intermediaries picked randomly, even if an intermediary is compromised, there's precious little the interceptor can determine about either the message or the pattern of communications.

NRL provides a prototype Onion Router (<http://onion-router.nrl.navy.mil/Prototype.html>) if you want to use the Net without revealing yourself. If you're not behind a firewall, you can make the Onion Router a browser proxy and visit sites without revealing your address or cookies. (All bets are off if your browser does ActiveX.)

In this age of Clipper chips, key escrows, and encryption controls, it's amusing to see this facility being provided by the Department of Defense (that is, if you trust NRL not to track usage of its Onion).

I also appreciated the page on onions in literature. 🕷️ 🕷️ 🕷️

**Top 100 Host Names • Internet Software Consortium •**  
<http://www.isc.org/ds/WWW-9907/firstnames.html>

Trying to decide what to name your baby? For a human baby, select a name like "Grant" or "Helena" from Eponym

(<http://student-www.uchicago.edu/~smhawkin/names/>), or check out alfabette zoope for unusual names ([http://www.zoope.com/k/k\\_names.html](http://www.zoope.com/k/k_names.html)).

If Santa left you a computer, the Internet Software Consortium will tell you the 100 most popular host names, which reveal not a trace of character beyond "mars," "venus," and "zeus." And you certainly ought to be able to do better than "cisco" or "gateway." (If you're too desperate for ideas, try the Christopher Siren's Myths and Legends page at <http://pubpages.unh.edu/~cbsiren/myth.html>.) 🕷️ 🕷️

**Kerberos: An Authentication Service for Computer Networks • USC-ISI •**  
<http://gost.isi.edu/info/kerberos/>

You don't want to name your kid Kerberos, because who wants to have to explain that they were named after the three-headed watchdog who guards the entrance to Hades. You probably don't want to name your computer Kerberos, either, unless you're just using it to run the Kerberos authentication system.

Kerberos is an authentication service. That is, Kerberos can be used by a server in a distributed system to "make sure" that someone professing to be, say, Santa, really is Santa and not a grinch planning to leave a Trojan Horse under your tree. It does this by providing a third-party (the Kerberos server), trusted by both the client and the server with their secret

keys (passwords). To communicate with the server, the client invokes the Kerberos service, specifying the desired server, and receiving both a time-stamped session key and a certification of the client's identity, all encrypted with the server's key. These certifications can then be sent to the server, which can decrypt them and be assured of the client's identity. The server and client can then use the session key to communicate securely.

Traditional approaches send raw passwords across networks. Kerberos encrypts all communications, ensuring that a network eavesdropper cannot obtain the information needed to forge another identity (beyond cracking the cryptography). (Of course, this doesn't protect you from corrupted workstations, Trojan horses that steal passwords, password guessing schemes, or a corrupted Kerberos server.) Kerberos is implemented with symmetric key cryptography (DES). With the public-key patents expiring, perhaps the next version will not be nearly so complicated.

The site includes a good overview of Kerberos in Neuman and Ts'o's paper (<http://nii.isi.edu/publications/kerberos-neuman-tso.html>); a dangling pointer to the Kerberos FAQ (really at <http://www.faqs.org/faqs/kerberos-faq/user/>); pointers to other Kerberos sites (check out in particular <http://www.contrib.andrew.cmu.edu/~shadow/kerberos.html>); and pointers to competing systems, particularly the European effort on Sesame (<https://www.cosic.esat.kuleuven.ac.be/sesame/>), which performs authentication and then some, at the minor cost of being a lot more complicated. (See <https://www.cosic.esat.kuleuven.ac.be/sesame/matsulf/kerbes.html> for a user's comparison of the two.) 🕷️ 🕷️ 🕷️



You'll find the Arachnoid Tourist this month at *IC Online*, and the archives include the hyperlinked past issues as well.

<http://computer.org/internet/arch.htm>