Macho Computing at Root of RSA Contest Flap

by James Glave

5:56pm 3.Mar.97.PST Last week's denial-of-service attack on machines participating in a contest to crack the RSA's 56-bit encryption key can be chalked up to processing envy and "macho computing," says a spokesman for the Canadian firm that was the main focus of the attack.

"Our supercomputer setup ran at over 10 million keys per second, while [another] large hardware vendor [a participant] could only muster 5 million keys per second," Michael Slavitch of Loran International Technologies told Wired News on Monday.

Loran's supercomputer was one of more than 10,000 machines participating in the RSA Data Security Secret-Key Challenge hosted by New Media Technologies. The machines are all working together to crack a 56-bit encryption key and demonstrate the ineffectiveness of US cryptography export laws.

The attacks on deckard.loran.com first began last Tuesday with threatening emails - with faked headers - ordering Loran to drop out of the contest. The mail was followed up with a SYN flood denial-of-service attack that evening. The attacker used spoofed IP addresses to hide the attack's origin.

On Thursday, the Loran machine was attacked again, along with those at New Media Laboratories, as previously reported. Slavitch told Wired News that New Media president Earle Ady said computers at Carnegie Mellon University had been hit, too. Thursday's attack prompted Loran to pull its supercomputer out of the contest.

Loran's team believes that the performance of its "sweat equity" machine - which was designed to verify the underlying technology of its Kinnetics network management system - deflated the egos of other participants. The machine is a loosely coupled system of 168 486-100 CPUs, eight Ethernet switches, 24 Ethernet repeaters, and six four-port routers.

The scoreboard of top 100 hosts participating in the contest includes universities such as Carnegie Mellon, as well as major hardware vendors including Sun Microsystems, Silicon Graphics, and IBM.

Another participant says Loran's theory is dubious. John Rumpelein of the Seattle-area ISP called MPL.NET pulled his machines out of the contest as soon as he heard of the syn flood attacks.

"A lot of people pulled out," said Rumpelein, a veteran of previous RSA contests who was participating under the linux@linuxnet.org group. He says the infighting and attacks emerged as a result of hostilities between contestants being played out on the #root Internet Relay Chat channel.

"There is also a lot of hostility toward the organizers, who refused to release the source code for the client," said Rumpelein. Contest organizers said they had to keep the source code secret to "protect everyone."

While Rumpelein said he is "waiting for a more serious group to organize a new RSA challenge," another participant, Steve Hill of IBM in the UK, said that owing to a series of client changes, the New Media Labs effort has become "an organizational nightmare."

"What had started off with the best intentions had spiraled into a 'my CPU is bigger than yours' contest, and then proceeded to get very nasty," said Hills in an email to Wired News.

"As far as we know we were never actually attacked and were certainly not involved in any attacks ourselves. It's a real shame certain dishonest people would ruin the contest for the many honest participants," Hills said.

Organizers say they are doing what they can to head off further server trouble. "We will use a set of caching proxies and round robin DNS to alleviate the performance bottleneck we are having with a TCP-based key server," said Christopher Stach of NetDox. "We will still be somewhat vulnerable to TCP syn flood attacks, but there isn't much to prevent that," he said.

Meanwhile, the contest continues - for now. "If people can't play nice, we will take our toys and go home," said Stach.

"I'm sure there are plenty of other people out there who are willing to deal with the big babies out there who are too insecure with their own product or with themselves," he added.