RSA Crackers Throw a Fit, Launch Syn Flood

by Kristi Coale

6:57am 1.Mar.97.PST When Earle Ady organized a group to tackle the latest RSA Data Security Secret-Key Challenge - crack a 56-bit encryption key - he never imagined that his own team would become his own worst security nightmare.

In the wee hours of Friday morning, Ady awoke with a big headache. His computers, and others among the 10,000 machines trying in unison to crack the RC5-56 key and expose the weaknesses of US encryption export laws - were falling victim to SYN flood attacks.

Ironically, the culprits were other members of Ady's team, hot to show that their hardware was the best.

"It's basically childish people who don't care about the underlying cause and worry more about their ranking," said Ady, president of New York-based New Media Laboratories.

In early February, using his own resources, Ady started working on the RSA challenges - an escalating series of contests to see how long it would take to crack increasingly stronger encryption keys.

But as the keys increased in complexity, he realized he needed more computing power. Within a matter of days, he had formed a team with a combined computing power of 5,000 machines. The team currently includes more than 10,000 machines, all working together to crack the latest key in the challenge, RC5-56.

On one of his machines, Ady kept a tally of how quickly each of the machines was working to crack the keys. From these results, he was able to generate a ranking of machines in terms of the number of key "spaces," or segments, they cracked. The machines highest on the list were considered the fastest.

And here lay the problem. Other team members were envious of those on the top of the list. Three or four of these lower-ranked members decided to launch an attack on Ady's ranking server, a problem which Ady fixed right away.

But other mischief followed. Some names at the top of the list, including large corporations, were targeted for SYN flood attacks - the servers were flooded with half-completed requests for data.

The team also includes university students and small corporations, some of which are hardware vendors using the experience to performance-test their machines. For some, a lower rating was an affront to their product.

"As much as I'd like to crack the key and show the government how weak [56-bit] encryption is, it's not worth it when corporate networks are being attacked," said a discouraged Ady.

Although Ady would not disclose the identity of the culprits, he hinted that one of them was a major hardware vendor. He was equally reticent about the names of the big corporations involved. "Some of them don't want [people] to know they're taking part in this," he said.

Though the attack slowed down his team's progress for a while Friday morning, Ady said it won't stop his efforts. He's busily writing a new piece of software to handle the stats and standings so those who wish to have their identities concealed may remain anonymous. Ady said he hopes to have it finished by Monday.

He hopes his whole team can continue. But if the participants can't play nice, then Ady said he'll shut down the whole operation.