-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

distributed.net completes rc5-64 project (list announcement)
september 25, 2002

RC5-64 HAS BEEN SOLVED!

On 14-Jul-2002, a relatively characterless PIII-450 in Tokyo returned the winning key to the distributed.net keyservers. The key 0x63DE7DC154F4D039 produces the plaintext output:

> The unknown message is: some things are better left unread

Unfortunately, due to breakage in scripts (dbaker's fault, naturally) on the keymaster, this successful submission was not automatically detected. It sat undiscovered until 12-Aug-2002. The key was immediately submitted to RSA Labs and was verified as the winning key.

So, after 1,757 days and 58,747,597,657 work units tested the winning key was found! While it's debatable that the duration of this project does much to devalue the security of a 64-bit RC5 key by much, we can say with confidence that RC5-64 is not an appropriate algorithm to use for data that will still be sensitive in more than several years' time. On the distributed computing front, however, the RC5-64 project clearly demonstrates the viability of long-term, volunteer-driven, internet-based collaborative efforts. The next time someone bemoans the public's short attention span or need for instant gratification you should remind them what 331,252 people were able to accomplish by joining together and working for nearly five years. distributed.net's RC5-64 project clearly shows that even the most ambitious projects can be completed by volunteers thanks to the combined power of the internet and distributed computing.

Ignoring artificially high numbers resulting from network difficulties, we completed 86,950,894 workunits on our best day. This is 0.12% of the total keyspace meaning that at our peak rate we could expect to exhaust the keyspace in 790 days. Our peak rate of 270,147,024 kkeys/sec is equivalent to 32,504 800MHz Apple PowerBook G4 laptops or 45,998 2GHz AMD Athlon XP machines or (to use some rc5-56 numbers) nearly a half million Pentium Pro 200s.

Over the course of the RC5-64 project, 331,252 individuals participated. We tested 15,769,938,165,961,326,592 keys.

We apologize for the latency in the announcement, but scheduling conflicts with RSA Laboratories and difficulties in reaching the winning participant (who has asked to remain anonymous) introduced the additional delay to the process.

Also, please consider joining us on SlashNET IRC on Saturday 28-Sep-2002 @ 21:00 UTC (5:00PM EDT) for an online Q+A session on the RC5-64 project and the future plans for the distributed.net network. Not only are we looking forward to moving on to RC5-72 but we're currently reshaping the framework of the dnetc architecture to better accommodate additional projects. We're hoping to attract some new and motivated partners with good ideas and a need for cycles.

Thanks to RSA Labs for continuing to offer challenges that reward distributed efforts!

For more information, contact:

* David McNett <nugget@distributed.net> +1-512-350-5038

References

http://www.slashnet.org/
http://www.rsasecurity.com/news/releases/pr.asp?doc_id=1400
http://www.distributed.net/rc5/

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.7 (FreeBSD)

iD8DBQE9lKZcgAekZNFUBFURAkYcAKCOTk63Bpi/8beOA/6GxOGi4/VqLwCeMeXB
M1zR4DccCqJ26YxUUrKyXOg=
=DP11
-----END PGP SIGNATURE-----