

Re: "Small" problem

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-08/1142.html>

From: Michael Amling (*nospam_at_nospam.com*)

Date: 08/16/03

Date: Sat, 16 Aug 2003 03:32:55 GMT

Gregory G Rose wrote:

> *[I'm replying to both Alex's and Mike's posts,*

> *having never received Mike's.]*

>

> *In article <W7a%a.732212\$ro6.15056543@news2.calgary.shaw.ca>,*

> *Alex Flanagan <spiffy43@hotmail.com> wrote:*

>

>> *Mike Amling wrote:*

>>>

>>> *You mean if two states for the same date hashed to the same value,*

>>> *and the wrong one is found first by the 0..255 loop?*

>

> *Yes, exactly.*

>

>>> *You can avoid this possibility by choosing a k for which it doesn't*

>>> *happen. 2**18 messages have to be checked to make sure than no two*

>>> *states for a given date produce the same hash. It should take only a few*

>>> *seconds on a PC to vet a given k.*

>

> *Not really; that will be true for any given*

> **date*, but you won't be able to choose such a k*

> *that will work for arbitrary dates.*

The plan (This not Luby-Rackov. This is the hash plan.) is to send the 26 least significant bits of the HMAC_k of (10-bit date concatenated with 8-bit state). Dates are allowed to be arbitrary only to the extent that they fit into 10 bits. A key can be vetted by comparing all 2**18 possible different hashes produced for a given k and rejecting k if there are any duplicates in the least significant 26 bits. How do you arrive at "Not really"?

—Mike Amling