

Re: [fw-wiz] strong passwords

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-07/0032.html>

From: Mikael Olsson (mikael.olsson@clavister.com)

Date: 07/10/02

From: Mikael Olsson <mikael.olsson@clavister.com>

To: miha@nil.si

Date: Wed Jul 10 12:51:12 2002

miha@nil.si wrote:

>

> *Now, I don't have my copy of Applied Cryptography ready, but isn't 50:50
> chance much too high? If I remember correctly it is more in the lines of:
> birthday attacks are possible, just not very likely, but finding something
> that hashes to the same value as a specific text/password is next to
> impossible (very hard).*

[trying to re-apply what i've forgotten --- remember I'm on vacation :)]

It's basically like this:

Laws of probability dictate that if you give a 64-bit input to a hash that produces a 64-bit output, there is a *_very good chance_* that there is at least one input that will produce the same output.

If this is not true, it isn't a one way function: it'd be a cipher.

Now, if you give the hash *_more_* than 64 bits of input, there's obviously going to be collisions, but that is to be expected.

65 bits input will have twice as many collisions as 64 bits.

66 bits input will have four times as many ...

Actually, it doesn't have to be 64-bit inputs, it can be any length input. Basically, what the hash function does is take an input and transform it into "a random output". So twist your thinking around into thinking "x balls has to go into y buckets", and you get:

For 50 balls going into 100 buckets:

- 30 balls alone in a bucket
- 15 balls sharing a bucket with one ball (single collision)
- 4 balls sharing a bucket with two balls (double collision)

[hash lookup tables are often designed with twice as many buckets as input items btw --- as you can see, the statistics look pretty good]

Re: [fw-wiz] strong passwords

Firewall-Wizards: Re: [fw-wiz] strong passwords

For 80 balls going into 100 buckets:

- 36 balls alone in a bucket
- 29 balls sharing a bucket with one ball (single collision)
- 11 balls sharing a bucket with two balls (double collision)

For 100 balls going into 100 buckets:

- 37 non-collisions
- 37 single collisions (hey, 50:50 :))
- 18 double collisions

So uhm.. yeah, i know, i'm probably confusing y'all. Let's see if I can turn it right again.

So, for all possible inputs to hash, you get, statistically speaking:

- 37% collision free inputs
 - 37% inputs that generate the same output as another input
 - and 18% inputs that generate the same output as TWO other inputs.
- And this is assuming that the hash is perfect.

NOW: if I've completely mucked up somewhere along my line of thought, someone please holler sometime real soon before I confuse everyone too badly :)

/Mike, blames it all on being on vacation

--

Mikael Olsson, Clavister AB
Storgatan 12, Box 393, SE-891 28 ÖRNSKÖLDSVIK, Sweden
Phone: +46 (0)660 29 92 00 Mobile: +46 (0)70 26 222 05
Fax: +46 (0)660 122 50 WWW: <http://www.clavister.com>
"It's July. I'm on vacation. Can't you tell? :)"