

Re: US Congress already discussing bans on strong crypto

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-09/5602.html>

From: Kris Kennaway (kris@obsecURITY.org)

Date: 09/18/01

Date: Mon, 17 Sep 2001 20:05:34 -0700
From: Kris Kennaway <kris@obsecURITY.org>
To: Scott Corey <Scott@bsdprophet.org>

On Mon, Sep 17, 2001 at 12:42:02PM -0500, Scott Corey wrote:

> *Michael Richards wrote:*

>>

>> *I think it would be just as effective if they were to pass a law
>> requiring all terrorist organisations to provide backdoor keys to
>> their encrypted communications.*

>>

>> *Since things like DES and RSA are so widely published there really
>> isn't a way to make these "go away". If you're planning on hijacking
>> aircraft and flying them into buildings, I don't think you will care
>> that much about a little law against sending PGP'd email.*

> <snip>

>

> *What makes you think there are no backdoors now?*

There's nowhere to put a "backdoor" in the RSA algorithm. There's room to put a backdoor in the DES algorithm, and in fact when the DES algorithm was under consideration back in the early 70's the NSA did request a change to the "S-Boxes" of the candidate algorithm submitted by IBM which was eventually accepted. This change may have seemed suspicious, until a number of years later when civilian cryptographers discovered the technique of differential cryptanalysis and realised that the NSA's changes were to improve the resilience of DES against that attack, which they evidently already knew about.

As for backdoors in other algorithms: well, that's why peer review of cryptosystems by trained cryptographers is so important. People spend their lives trying to break cryptosystems. If you listen to their recommendations, you'll do pretty well.

Kris

FreeBSD–Security: Re: US Congress already discussing bans on strong crypto

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd–security" in the body of the message

- application/pgp–signature attachment: [stored](#)