

Re: Meganet on Cryptogram again

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/1447.html>

From: Mxsmanic (*mxsmanic_at_hotmail.com*)

Date: 09/18/03

Date: Thu, 18 Sep 2003 11:18:41 +0200

Scott Contini writes:

- > *You CAN discount an algorithm because it has NOT BEEN*
- > *PUBLICALLY ANALYZED BY EXPERTS IN THE FIELD.*

So all the most important secrets of the USA are being protected by discountable algorithms? After all, they haven't been publicly analyzed by experts in the field.

- > *Unless, of course, you want to be optimistic and HOPE*
- > *that maybe this is the new great thing, even though it hasn't*
- > *proved itself in anyway. But quite frankly, if you're*
- > *so optimistic in the first place, then why should you*
- > *think anybody will try to eavesdrop on your data anyway?*
- > *In that case, maybe you do not need any security at*
- > *all!*

You're describing a false dilemma. It's not a choice between secure and insecure, it's a balance between potential loss and the cost of security. A cryptosystem need only provide enough protection to make its compromise too expensive in relation to the value of the secrets it protects. It doesn't have to be unbreakable.

- > *They are attempting to side-step the analysis process.*

What analysis process? Nobody has offered to attack their algorithm, from what I understand.

- > *Nobody has posted a PUBLIC attack on their algorithm. That does not*
- > *mean it has not been attacked and broken.*

That is true for all algorithms, so it does not work against Meganet's algorithm in particular.

- > *You submit your algorithm to the security community to have*
- > *it publically analysed in order to prevent such huge blunders*
- > *before they happen. Meganet has not done this.*

sci.crypt: Re: Meganet on Cryptogram again

They don't have to, and perhaps they shouldn't. It seems that not revealing the algorithm is itself sufficient to prevent anyone from trying to attack it.

Cryptanalysts may be spoiled. Sure, it's nice to have the algorithm in front of you, but in the real world, adversaries don't provide you with copies of their cryptosystems in order to facilitate your analyses. And if you refuse to attack any system for which you don't have all the manuals, then any undisclosed system is unbreakably secure—security by obscurity works.

--

Transpose hotmail and mxsmanic in my e-mail address to reach me directly.