

Re: Ce-Infosys Compusec password strengthness

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-04/2794.html>

From: Tom St Denis (tom_at_securescience.net)

Date: 04/30/04

Date: Fri, 30 Apr 2004 11:58:15 GMT

Baratt wrote:

>>*Email the tech support?*

>>

>>*Tom*

>

>

> *The reply is that they don't clearly understand what I mean with*

> *"strengthness". Sure, my english is not really good but I think isn't*

> *really hard to understand.*

> *But, in general:*

>

> *If you use a 256 bit encryption algorithm (say, AES256), should you*

> *use a password \geq 256 bit to achieve the optimal security?*

Generally yes. Though there are other reasons to use AES256. Marketing is a good one. See big-number theorem states that a poorly designed product + one blue button + bignumbers == profits.

Tom