

Re: Cryptography problem

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-06/0307.html>

From: Lassi Hippeläinen (*lassi.hippelainen_at_welho.organized.invalid*)

Date: 06/26/04

Date: Sat, 26 Jun 2004 08:40:14 +0300

Eugene Mayevski wrote:

- >
- > *Hello!*
- > *You wrote on Wed, 23 Jun 2004 16:19:59 GMT:*
- >
- > *DH> Third, I need to stop automation software from entering bogus searches*
- > *DH> programmatically to gain incentives for the hacker.*
- > *DH> So, it doesn't necessarily have to be my software, as long as the*
- > *DH> request is authentic and not automated (actually entered in real time*
- > *DH> by a human at a keyboard). But, I believe the only way I can assure*
- > *DH> the later it by being the client.*

Looks like a beginning of a threat model. Are only external enemies your worry, i.e. do you trust your true clients?

- > *Then you need to look at different methods of distinguishing the human user*
- > *from automated software. The most popular method, as you know, is asking the*
- > *person to enter some text shown as an image.*
- >
- > *Unfortunately this seems to be the only way to protect from automated*
- > *clients.*

Unfortunately there is a man-in-the-middle workaround to graphic challenges. The attacker needs only to install a service that has a constant supply of innocent human users. The challenge (text as image) can then be relayed to a real person, and the response is relayed back to the original challenger.

— Lassi, getting back to summer vacation...