

# Re: Defeating keyloggers with encrypted one time passwords (a patent spoiler?)

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-12/msg00510.html>

---

- *From:* Sam <CPSCSam@xxxxxxxxxx>
  - *Date:* Mon, 12 Dec 2005 19:31:39 GMT
- 

Juuso Hukkanen <juuso12\_2003@xxxxxxxxxx> wrote in  
[news:12puo11ruiq7j2oeuos4pagcn44j498sqd@xxxxxxxx](mailto:news:12puo11ruiq7j2oeuos4pagcn44j498sqd@xxxxxxxx):

- > A simple idea for enhanced password protection!
- >
- >
- > -----BEGIN IDEA (don't mix with IDEA) -----
- >
- > The only maintainable answer (to password protection) are the ONE
- > TIME PASSWORDS and more precisely an A4 sized paper full of them and
- > folded up into the valet. Ok, that leaves a problem what if someone
- > steals the wallet, or worse... borrows the paper and copies it. The
- > solution for eliminating (most) a risk, caused by loss of the password
- > paper, is the following:
- > 1) The password paper (or similar) is made contain slightly encrypted
- > passwords! i.e. all the passwords on a paper are slightly erroneous,
- > but just so little that the user can easily remove the encryption.
- > 2) The encryption method for the papers passwords can be decided by
- > the user of the provider of the passwords.
- > 3) Optionally the paper containing the encrypted paper can be set to
- > contain the information for easy removing the (light) encryption. In
- > such case the paper could contain for example a dashed line which
- > would say a scissors away these decryption instruction – and destroy
- > them after you have memorized and learned the decryption instructions.
- >
- > Example decryption instructions... TO DECRYPT:
- > – remove two first character of each password
- > – remove the third character of each password
- > – Switch the first and last character of each password
- > – change the case of all letters
- > – switch the fourth and fifth character of each password
- > – add 1 to every number character (9 becomes 0)
- >
- > -----END IDEA (don't mix with IDEA) -----
- >
- > Dear ALL READING PROFESSIONAL, hope you remember this, in case someone
- > seeks a patent for a similar system / method.
- >

Re: Defeating keyloggers with encrypted one time passwords (a patent spoiler?)

- > Regards
- > Juuso Hukkanen
- > (to reply by e-mail set addresses month and year to correct)
- >

The paper method also works well without the decryption instructions. Just have the page with the passwords numbered. The server has the hash for each key (and its salt). When the person visits the site it will select a password at random (well, close to random) and asks for password number #..., reduce the likelihood that the thief, who's only take one password, can use it to obtain access we do not allow the password being asked for to change for some period (10 minutes?). This helps against the attacker knowing password #39 and then hitting "Reload" until it prompts for password #39. And of course after a password is used it will never be prompted again while maintaining the date and time of when it was used.

All in all, you guys have actually sold me on this method. Forces employees to use a strong password rather than the conventional "God", "password" and "sex". Only thing is I know that they'd keep the list taped to the side of their monitor or in the top drawer.

---

- *Follow-Ups:*

- ◆ [Re: Defeating keyloggers with encrypted one time passwords \(a patent spoiler?\)](#)  
◇ From: Juuso Hukkanen

- *References:*

- ◆ [Defeating keyloggers with encrypted one time passwords \(a patent spoiler?\)](#)  
◇ From: Juuso Hukkanen

- Prev by Date: [Re: Private Post](#)
- Next by Date: [Re: Rather Newb-ish Question](#)
- Previous by thread: [Re: Defeating keyloggers with encrypted one time passwords \(a patent spoiler?\)](#)
- Next by thread: [Re: Defeating keyloggers with encrypted one time passwords \(a patent spoiler?\)](#)
- Index(es):
  - ◆ [Date](#)
  - ◆ [Thread](#)