

Re: 2 security issues

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2001-12/0068.html>

From: bugtraq@t-swat.com

Date: 12/14/01

Date: Thu, 13 Dec 2001 20:36:51 -0800

To: Focus on Linux Mailing List <focus-linux@securityfocus.com>

From: "bugtraq@t-swat.com" <bugtraq@t-swat.com>

At 12:12 PM 12/12/2001, mike ledoux wrote:

> > *Just remember that anything that can be automatically done, can be*
> > *automatically "un-done". That's like locking the door but leaving the key*
> > *under the mat.*

>

>*I don't believe that is true in this case. For GPG to encrypt to a key,*
>*it only needs the public key; to decrypt it needs both the private key*
>*and the passphrase. As long as the machine doing the encrypting doesn't*
>*have a copy of the private key, it should be quite difficult for someone*
>*to automatically undo the encryption.*

>

>*If he were using symmetric encryption, then I'd agree with you.*

I seem to have typed before I thought and really didn't respond appropriately to that particular question. In other words, it didn't come out right. :)

I've consulted on a number of e-commerce projects where developers were under the impression that by encrypting things like credit card numbers and then storing those encrypted values in the database of choice, that somehow made that information secure.

What they failed to appreciate was the fact that they had a function that, when called, went out and retrieved that encrypted data from the database, un-encrypted it, and then sent it off to the credit card processing service.

The key point was that you didn't have to crack the encrypted data, you just had to call the function that did it for you; all required keys and passphrases were included within that function. So, if the box was hacked, they'd have given up all those CC numbers. In this case they had indeed locked the door but left the key under the mat.

So, if I were to re-state my previous statement, I'd have to say that as far as data security is concerned, it is important to look at the entire system as a whole to see how secure the data is... don't just concentrate on one small part of it and lose sight of the rest.

SecurityFocus Linux: Re: 2 security issues

\$0.02

...jeff

- *Previous message:* [Robin Lynn Frank: "Re: 2 security issues"](#)
- *In reply to:* (deleted message) [mike ledoux: "Re: 2 security issues"](#)
- *Next in thread:* [Dave Vehrs: "RE: 2 security issues"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)