

## Re: mlock(1)

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-09/9157.html>

---

**From:** Pavel Machek ([pavel\\_at\\_suse.cz](mailto:pavel_at_suse.cz))

**Date:** 09/30/04

Date: Thu, 30 Sep 2004 21:52:28 +0200  
To: Andrea Arcangeli <[andrea@novell.com](mailto:andrea@novell.com)>

Hi!

> > *Actually if your cipher is not resistant to known plaintext attack,*  
>  
> *AFIK the only way to make it resistant to a brute force is to make it*  
> *slow, like adding lots of bits of salt.*

No. If you want it resistant to brute force, use big key. Actually 128bit should be enough.

If user's password has at least 128 bits of entropy, you should be safe, too.

salt only helps with "lets create 1TB of all common encrypted passwords" attack.

> *My point is very simple, that is if you leave a zero as part of the API,*  
> *then you're making things less secure.*

This is same as saying that starting encrypted email with "Hi!" is bad idea. It is not. Don't worry about brute-force, it is not practical. (Okay, you probably should not limit password length to 8 chars).

Pavel

--

64 bytes from 195.113.31.123: icmp\_seq=28 ttl=51 time=448769.1 ms

-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to [majordomo@vger.kernel.org](mailto:majordomo@vger.kernel.org)

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>