

Re: [PATCH] Delete cryptoloop

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-07/6339.html>

From: Matt Mackall (mpm_at_selenic.com)

Date: 07/31/04

Date: Fri, 30 Jul 2004 21:05:34 -0500
To: David Wagner <daw@cs.berkeley.edu>

On Fri, Jul 30, 2004 at 05:44:24PM -0700, David Wagner wrote:

> > *But we identified more problems (I don't if these are all real issues).*
> > *Assuming the attacker has access to both plaintext and the encrypted*
> > *disk. (shared storage, user account on the machine or something)*
> [...]
>
> *Yes, there are a host of potential attacks in this scenario. That's why I*
> *wrote that, if you find yourself in this threat model, it would be prudent*
> *to assume that the current disk encryption scheme can potentially be*
> *defeated. Does anyone care about these threat models? From the design,*
> *I had assumed that no one cared, but if they are relevant in practice,*
> *then it might make sense to investigate additional defenses.*

Here's a probable scenario: encrypted mail spool in maildir format.
Attacker can send mail of his choosing and then later capture the
machine with the hope of breaking in.

Ideally, we'd ship a requirements and specification document that
describes the security trade-offs of cryptoloop/dm-crypt in some
detail. There are way too many unstated assumptions here.

--

Mathematics is the supreme nostalgia of our time.

-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in
the body of a message to 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/>