

Re: Security Flaw in Popular Disk Encryption Technologies

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2008-02/msg00369.html>

- *From:* "Igor Mozolevsky" <igor@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 24 Feb 2008 15:16:54 +0000
-

On 24/02/2008, Bill Moran <wmoran@xxxxxxxxxxxxxxxxxxxxxxxx> wrote:

"Igor Mozolevsky" <igor@xxxxxxxxxxxxxxxxxxxx> wrote:
>
> On 23/02/2008, Brooks Davis <brooks@xxxxxxxxxxxx> wrote:
>
>>
>> You should actually read the paper. :) They successfully defeat both
>> of these type of protections by using canned air to chill the ram and
>> transplanting it into another machine.
>
> Easy to get around this attack – store the key on a usb
> stick/cd/whatever and every time the OS needs to access the encrypted
> data the key should be read, data decrypted, then key wiped from the
> memory; or have the daemon erase the key from memory every T minutes
> and re-acquire the key at next access attempt...

This is only effective if the sensitive data is infrequently accessed.
If the unit is asleep, then software isn't running and it's not possible
to kick of a timer to clear the memory, so it doesn't even start to
solve that problem.

IMO the possibility of such attack is so remote that it doesn't really
warrant any special attention, it's just something that should be kept
in mind when writing "secure" crypto stuff...

freebsd-hackers@xxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-hackers>

To unsubscribe, send any mail to "freebsd-hackers-unsubscribe@xxxxxxxxxxxx"