

Re: [Full-disclosure] Gutmann's research paper today

# Re: [Full-disclosure] Gutmann's research paper today

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-02/msg00117.html>

---

- *From:* Frank Knobbe <[frank@xxxxxxxx](mailto:frank@xxxxxxxx)>
  - *Date:* Tue, 07 Feb 2006 10:16:35 -0600
- 

On Tue, 2006-02-07 at 10:07 -0500, Valdis.Kletnieks@xxxxxx wrote:

One place where "random scrubbing" falls down is the requirement to \*verify\* that the blocks were written. If you wrote a disk full of zeros, it's a trivial matter to read it back and verify that all the bytes are zeros. If you wrote a whole disk of pseudo-random, then you have to regenerate the entire pseudo-random data stream in order to compare it....

Shouldn't you be able to do that cluster by cluster? Grab 1024 or random, write it, then read it and verify?

Alternatively, more stream based, you could dd /dev/random, tee that to the drive and pipe the other stream into md5. Take note of the hash. At the end, dd the drive into md5 and compare the resulting hash.

I'm performing backups where the stream is tee'ed to the drive and into md5 for hash creation. Works great with tapes, should work for drives too.

Cheers,  
Frank

—

It is said that the Internet is a public utility. As such, it is best compared to a sewer. A big, fat pipe with a bunch of crap sloshing against your ports.

***Attachment: [signature.asc](#)***

*Description:* This is a digitally signed message part

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Re: [Full-disclosure] Gutmann's research paper today