

Re: DRAM data persistence

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2007-07/msg00514.html>

- *From:* MooseFET <kensmith@xxxxxxxx>
 - *Date:* Thu, 05 Jul 2007 06:18:38 -0700
-

On Jul 5, 4:37 am, krw <k...@xxxxxxxx> wrote:

In article <slrnf8pfm2.5eds.dha...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, dha...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx says...

Nico Coesel wrote:

Any modern OS clears the memory before freeing it for use by other tasks.

This is not correct.

This is very correct otherwise there would be a huge security hole.

Name ONE operating system that does this. Besides, if I were to write a program for which leftover RAM (or swap) content was a security hole, I'd clear that memory myself before releasing it, rather than relying on your imaginary OS feature.

MVS, and I believe any other OS that is B2 rated.

Yes, I think you are right. IBM's MVT didn't and this was the source of many security problems. This was because they assumed that anything in memory that had a key of zero was theirs but didn't enforce it. You could make a look alike for an OS data structure and

Re: DRAM data persistence

free it then quickly use it. This way you could fool the OS into jumping to your code. I can imagine IBM nailing that door shut and bricking it up.

.