

Good afternoon,

I enjoyed reading this.

The last part regarding the warning on the TrueCrypt webpage stood out to me, as although I had seen this on the website, I didn't think much of it. Upon reflection, you're absolutely right that this should be a very visible warning about whether TrueCrypt should be recommended or not. Surely, if they cannot secure their website, how can we trust them to secure sensitive data?

Leaks from kernel stacks, which you highlight in your opening, are simply unjustifiable when securing data. Pairing this with the weakness to brute force attacks, which aren't really sophisticated, then you have an easy way to access this information.

Overall, I strongly agree with what you have stated.