

Re: House on Fire... Do You Rescue the Computer?

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2008-04/msg04166.html>

- *From:* Keith M <keithvz@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 26 Apr 2008 16:46:48 GMT
-

John Tserkezis wrote:

- > Ah, and that's where the crunch is. <snip>
- > Today we're talking about speeds and internet accessibility that is
- > taken for granted in the US, is a special case here. Bang for buck wise
- > at least.

My real point was that you can't ignore a class of 300+ million people and claim that online backup is useless to them because other places don't have fast/unlimited internet access. I think the UK also has reasonably priced all-you-can-eat. This is a more recent development. As far as China/India/Japan -- I have no idea.

You have \$5 cable accounts?

Actually the mozy.com backup account is \$5, my internet account is \$45.

My internet access is 2mbps/15mbps for about \$45 month. They are upgrading us to 5mbps/20mbps for free soon.

"Free*" is treated with suspicion here. Note the asterisk.

Well sure. No such thing as a free lunch (I actually get a free lunch every day at work..... so hrrm..) Anyways, let me put it this way: there is no additional charge for an upgrade in bandwidth.

I have a pessimistic view of useful encryption keys verses practicality of using them on a regular basis and keeping the keys secure at the same time.

Good encryption is hard. Long keys are hard to remember. However, I'm particularly anal about using good keys.

Re: House on Fire... Do You Rescue the Computer?

Same here, but it's all local. I get instant (fast) access to files too. Important when I'm doing map image processing work. My bandwidth would get eaten up quite quickly with the larger files and the frequency they get updated.

Well sure. I actually rarely access my files on mozy. Although I've tested it to make sure it works properly, mozy for me, is a \$5/month worst case insurance program. So if my hard drive fails, I don't lose anything important. Mozy encourages good backup habits because its automatic. If my hard drive failed this afternoon, changes I made this morning would already have been backed up.

With 1mbps of upload bandwidth, it really is sufficient for most things I do. My only real storage-intensive tasks are storing digital photos (large 20mb RAW files), and then the subsequent editing of them. Even I offload a flash card to the PC, mozy can have those files uploaded to their servers in at most a few hours.

Incidentally, mozy tops out at about 10gb/day uploads (that's 1mbit/s * seconds in a day). It's really sufficient because I rarely cause 10gb of change per day to my system — so the system is almost always fully backed up. (excluding warez/movies/downloads that can just be re-downloaded)

Note that downloads are much faster than 1mbps. And mozy has multiple interfaces to get the data. The most convenient are the network-drives which allow you to copy files directly from their servers to your machine. They mimic your drive/drive structure, so it's as easy as accessing local files (but of course slower)

I had a discussion with a colleague some time back about encryption.

His point was existing algorithms are useless, because GovCo (or whoever you perceive as the bad guys) can setup software or hardware solutions to decrypt existing known algorithms. A proprietary algorithm will take longer.
My point was if encryption was not already your primary game, don't bother because it'll be weaker than what's already existing now anyway.

I've come to the conclusion that both sides have enough merit not to trust either. So I don't.

Without questioning your source, the modern, existing algorithms are secure enough against a brute-force attack. The people over at sci.crypt would probably have a field day with this conversation, and I'm trying not to incite violence here. :)

1> The bigger the adversary, the better your encryption had better be.

2> No one is brute forcing any modern key sizes. The search space is too large and dedicated computers/processors/boards don't even come CLOSE. There's the whole discussion of the amount of memory, cpu time, number of atoms in the universe, etc.....Except for maybe 56/64-bit DES, brute force attacks are useless unless you can reduce the search space CONSIDERABLY (and thereby break the algorithm)

3> If your data is important enough, the people will use rubber-hose cryptanalysis, and that usually works. No high-level math required.

4> It's impossible to put a metric on how secure something is, peer review and time are the only things that help.

Re: House on Fire... Do You Rescue the Computer?

5> Your friend has it backwards. Proprietary algorithms are almost always less secure than peer reviewed publically released algorithms. It's the number of smart eyes on the algorithm that can help determine ways of attacking it.

6> A keylogger physically or electronically installed will defeat the best encryption. As will a small camera surreptitiously placed....

Normally, you've really got to piss someone off before anyone is going to throw the kinds of resources needed to attack your encrypted data.

There are some really really scary ways of getting passphrases. Like the research where someone can record the SOUND of the keystrokes and determine which key was pressed. Or the EMI/RFI off the equipment. Or rebooting a secured computer with a usb->key that extracts the contents of memory, and getting the encryption key from memory, and so on. Often times there are back/side doors to achieve the same result. Like say the IMPLEMENTATION of the algorithm is broken. The famous example, I think, is WEP security for wireless. IIRC, they re-used the Initialization Vector, or the IV was easily guessable.

Good encryption is hard.

Keith

.