Bruce Schneier

Schneier on Security

A blog covering security and security technology.

« Friday Squid Blogging: Plush Squid | Main | New Siemens SCADA Vulnerabilities Kept Secret »

May 23, 2011

Dropbox Security

I haven't written about Dropbox's security problems; too busy with the book. But here's an excellent summary article from *The Economist*.

The meta-issue is pretty simple. If you expect a cloud provider to do anything more interesting than simply store your files for you and give them back to you at a later date, they are going to have to have access to the plaintext. For most people -- Gmail users, Google Docs users, Flickr users, and so on -- that's fine. For some people, it isn't. Those people should probably encrypt their files themselves before sending them into the cloud.

EDITED TO ADD (6/13): Another security issue with Dropbox.

Posted on May 23, 2011 at 6:47 AM • 63 Comments

To receive these entries once a month by e-mail, sign up for the Crypto-Gram Newsletter.

Comments

In the words of the immortal Joe Bob Briggs, "I'm surprised I have to explain these things to you."

Posted by: bkd69 at May 23, 2011 7:00 AM

The specific issue is that Dropbox lied about their ability to access the clear-text.

While it's obvious that deduplication across different accounts can not work without direct access to the plain text to you and me, most people do not even begin to understand the underlying issues.

That Dropbox lied to them, on purpose, is the issue.

Posted by: Richard "RichiH" Hartmann at May 23, 2011 7:15 AM

When researching Dropbox during a POC, I had contacted Dropbox sometime mid last year and asked them specifically who had ADK's to the data. They refused to respond stating that they cannot elaborate more on anything not disclosed in their privacy policy.

There is some debate on whether they were intentionally deceitful or just using marketing finesse. With the response I received, it was nearly an admission (to me anyway) that the data owner was not the person capable of decrypting the data.

Posted by: Justin at May 23, 2011 7:34 AM

What Richard said. They lied, confusing both lay people and computer-savvy folks.

It's not about expectations, it's about deliberate mis-information.

It is easy now to say "oh, you can't expect a cloud provider to do the right thing". But why the heck not?

V.

Posted by: VidKid at May 23, 2011 7:41 AM

I'm using a truecrypt encrypted volume on top of the dropbox service. The password was chosen by the software and it's an almost truly 256 bit ascii password. They can copy the volume as much as they want, I just don't care... :)

Posted by: Gianluca Ghettini at May 23, 2011 7:43 AM

From the Economist article it appears that whilst Dropbox may in some of their marketing blurb said they could not access the data, it appears that they where fairly honest about it when talking to customers right from the outset.

If this is true then Dropbox join the legions of other advertisers who make claims about a product.

However what I find really objectionable is the comment of Nathaniel Borenstein given and linked to at the end of the article,

"... need for privacy -- most often because they are breaking either a just or unjust law -- need..."

When are we going to get over the false assumption that "most" people are some kind of criminal simply because they wish to maintain in the digital world what many take for granted in the physical world which is not to make our personal business to all and sundry.

As Phil Zimmerman and many others have pointed out we send letters for the majority of our personal bussiness and usually only send post cards with the obligatory "wish you where here" from holiday (as a warning we are going to bore the recipient rigid with two hundred "holiday snaps" very very soon).

Posted by: Clive Robinson at May 23, 2011 7:51 AM

I looked at DropBox some years ago and decided not to use them as they didn't support private encryption keys which is really no encryption at all. Of course there are work arounds using Truecrypt and other tools to manually encrypt data before it is synced. I wouldn't say they lied about this but they were "economical with the truth". They aren't alone in this. A lot of services, including 'secure' file delivery and e-mail services, are misleading about the nature of the encryption they provide. There are alternatives to DropBox such as JungleDisk (a division of RackSpace) and SpiderOak that offer much better security.

The other issue with Dropbox is that there was a serious authentication problem. This is discussed here: http://dereknewton.com/2011/04/...

Posted by: AlanS at May 23, 2011 7:52 AM

About the inherent conflict between who can share and the security of the encryption - things are not so

clear cut.

For a while, my company tried to provide a service somewhat similar in audience to DropBox (this service is no longer offered to the public). We were focusing mostly on secure storage, but needed to handle small modifications to large files efficiently.

We ended up developing our own encryption solution (available as open source) called rsyncrypto. If you're interested in the details, you can get it from the project's home page - http://rsyncrypto.lingnu.com.

As far as analysis goes (and I'm sure mine is neither perfect nor objective), you give up some of CBC's known security in exchange for more efficient delta transfers.

My point is that you can encrypt (and keep the keys secret) on one hand, and yet provide more than just dumb file storage on the other, but you will have to give up something in the process.

Shachar

Posted by: Shachar Shemesh at May 23, 2011 8:04 AM

I think if you look at how this blew up for them. It started with Newton's post about the authentication issue. Dropbox staff dismissed that as a non-issue initially and that annoyed a lot of people. Critics moved on to the encryption issue which was actually well known even if the information posted on their website was misleading. There are many posts going back several years discussing how to use Truecrypt to better secure Dropbox data and Dropbox even modified it's software to work better with Truecrypt.

Posted by: AlanS at May 23, 2011 8:14 AM

@Clive Robinson - excellent post.

About the outrageous comments you cite, from NB elsewhere... FOLLOW THE MONEY! His staggering position will only be held by someone who makes money from discovery, or by selling products that boost discovery. Bet on it.

Posted by: jack at May 23, 2011 8:53 AM

@Gianluca Ghettin Does dropbox have to sync the entire truecrypt volume every time you make a change to it?

Posted by: Zach at May 23, 2011 9:43 AM

I don't understand what all the fuss is about. Yes the data is encrypted, on a SAN. Just like most cloud providers. They cannot provide access to data they don't have access to.

As for shared files, anyone who's used dropbox would know they were doing this (or something similar) based on the fact that shared files exist 'in' every user's Dropbox space that has access to them. They're not just sitting in one person's box and sharing out links...they're sitting in the cloud and even the owner just gets a link.

Posted by: Captain Obvious at May 23, 2011 9:52 AM

@Clive "need for privacy -- most often because they are breaking "

If you're not doing anything wrong what do you have to hide?

so. Clothing.

Looking at my fellow Americans? I've got to believe - a lot!

Posted by: BF Skinner at May 23, 2011 10:32 AM

They don't do encryption, and if they did then unless the encryption was in the client and open source then you still wouldn't trust it.
To an extent - so what? I have stuff in dropbox that is confidential and I encrypt it myself. There are websites I visit where I use ssl - I don't insist on a quantum-crypto secured sealed leased line from the telco to read bruce.

The difference is that Dropbox went from the 'well in theory the telco could monitor all your traffic' to actively checking all uploads, even inside zipped tars, for any content they disproved of. In this case the file sharing software's source.

Posted by: Nobodyspecial at May 23, 2011 11:20 AM

Author of the Economist piece, here. Thanks for the link. Also glad to see nuanced discussion of the issue here (no surprise).

I scrupulously avoided accusing Dropbox of lying, because the record makes it clear that whenever asked in the company's open forums whether they had access, they said yes (in varying ways). To state that Dropbox lied or even intentionally misled, one would need to see some kind of pattern: either providing the same incomplete information in forum responses, false statements to the media, or never responding to questions whatsoever.

The bigger is, as many commenters here point out, making a decision about where the key to your data lies: who possess it, who has access to it.

@Clive: I think you read Mr Borenstein's words the wrong way around. He wasn't stating that privacy is needed because most people are engaged in criminal acts (whether against just or unjust laws). Rather, that those that are knowingly engaged in acts that could be seen as criminal by the state are the ones who should take the greatest care in protecting their data.

@Zach: The TrueCrypt volume looks like a monolithic file to Dropbox, but I have read in various forum posts that Dropbox's indexing routine, which examines changed blocks, seems to work fine with TrueCrypt. Dropbox takes a while (one person reported 5 to 10 minutes with a 6 GB TrueCrypt volume) to examine hashes and figure out the differences and upload just those. I'd love a file-by-file on-the-fly encryption system, myself.

Posted by: Glenn Fleishman at May 23, 2011 11:31 AM

@ Shacha,

"As far as analysis goes (and I'm sure mine i neither perfect nor objective), you give up some of CBC's known security in exchange for more efficient delta transfers"

As a first aproximation, the way around the issue is to take a leaf out of the NAS etc world with "snapshots" and journaling. Just use the last "whole" snapshoot sent up and tage the diffs on the end. So the majority of the cipher chaned image (file or partition/container) remains the same, the end contains the "journal updates". Rsync etc should see only these changves at the end and update those.

However there are a number of other issues you need to address as well but.... There realy is not space to list even a few of them (not without upsetting the other readers).

Posted by: Clive Robinson at May 23, 2011 11:53 AM

I had an idea about creating a cloud RAID-like service that stripes your files over multiple independent cloud services using some variant of Drobo's Beyond-RAID file-based RAID algorithm. That way no one service has all of any one file and, if any of them go down (looking at you Amazon!), you can still access your files using the parity. Throw in a little encryption and I think you might have a very compelling product.

Posted by: Justin Mitzimberg at May 23, 2011 11:53 AM

There's a similar problem with the popular mint.com finance service. In order for it to sync with your bank accounts, they need to themselves store your login credentials with your bank. I suppose that's fine, if you know what you're getting into, but their claim is:

Mint is a "read-only" service. You can organize and analyze your
finances, but you can't move funds between–or out of–any
account using Mint. And neither can anyone else. (https://www.mint.com/how-it-works/security/)

Mint itself may be read-only, but they deliberately gloss over the fact that, if their system were compromised, attackers could get your bank credentials. An attacker with access to your bank credentials can do anything that your banks allows you to do online. Depending on the bank in question, this could absolutely include transactions which aren't exactly "read-only", to put it mildly.

Posted by: dob at May 23, 2011 12:02 PM

@Gianluca Ghettini: "They can copy the volume as much as they want, I just don't care..." I lose deniability of TrueCrypt hidden volume
https://www.usenix.org/events/hotsec08/tech/full_papers/czeskis/czeskis_html/

@Glenn Fleishman: "I'd love a file-by-file on-the-fly encryption system, myself." Too weak your you have small usual files (cvsroot file in CVS directory, ...)

Posted by: youlose at May 23, 2011 12:46 PM

Basic data security knowledge is not hard for the average person to understand, -if- couched in terms that are understandable.

Once it is pointed out to them, most ordinarily prudent people will be able to intuit the differences between their security requirements for "data at rest" when compared with "data in motion." Key management concepts are less easily graspable by the lay person, but if simplified in terms of access, ownership, and control, can be understood.

But enlightenment of the ignorant requires these be pointed out, and openly discussed. There's the rub.

Dropbox touts their key differentiators -- sychronization, and sharing.

Security? It appears to me that security is something of an afterthought, or lower down on the list in priority. Key management, ownership, and has bitten them fairly badly, if negative press is an indicator.

Posted by: jggimi at May 23, 2011 1:08 PM

@youlose: "Too weak your you have small usual files (cvsroot file in CVS directory, ...)" I don't organize that sort of thing in Dropbox, though. I'm thinking about my non-usual files.

You're concerned because usual files can be used to crack the key?

Posted by: Glenn Fleishman at May 23, 2011 1:20 PM

I believe the issue with the FTC complaint was that DropBox was deduplicating files. Christopher Soghoian claimed that they could not do that unless they could see the files. His accusation was that they were doing this to save on paying for storage, hence they were able to potentially undercut competitors who were making the same claim as DropBox (that they could not see the files) and were actually being truthful.

That wouldn't be an issue if DropBox had not claimed--or at least strongly implied--that they could not access your files. The statement that "all files...are inaccessible without your account password" would lead people to believe that they couldn't access your files (that statement has now been removed from their Web site).

I reviewed DropBox before using it and got the clear impression that they could not decrypt my files. I'm very glad now that I encrypted anything important before it ever left my computer.

The statement that files cannot be accessed without your password when they can in fact access them without your password is a blatant lie. There's nothing truthful about it. Needless to say, now I'm researching alternatives to DropBox.

Sources:

http://paranoia.dubfire.net/2011/04/...

http://www.wired.com/threatlevel/2011/05/...

Posted by: josh at May 23, 2011 1:33 PM

@gianluca:

"The password was chosen by the software and it's an almost truly 256 bit ascii password. "

Where does truecrypt choose a password??

Truecrypt gives a choice of allowing it to randomly generate a keyfile that you can use with a password.

I also use a truecrypt container for 'cloud backup', and use a random truecrypt generated file.

(i gave the file stored in the 'cloud', a .exe ending,
[can be done with truecrypt, just ignore the error message about .exe files ;-) btw, for some reason, it only gives this error message after successful decryption])

btw:

password suggestion;

[1] generate a gnupg key and encrypt anything to this key, and store the file in a safe place

[2] decrypt the file using the gnupg option of
--show-session-key

[3] copy the 64 character session key as your truecrypt password,
and let the 'cloud' merrily spin its wheels and resources trying to crack it

Posted by: vedaal at May 23, 2011 2:11 PM

I think all of the issues brought up are indicative of something we have all heard before, defense-in-depth. Why would anyone rely on a cloud-based (or any other really) vendor to protect their data (password protected, encrypted, whatever)? Another issue, how do you know that they are protecting your password? Even if you choose a 1k char password, if they store it in plain text, it is not worth the time it took to copy/paste. It only really protects you from bruteforcing, but not from someone stealing the db.

Posted by: No1nparticular at May 23, 2011 2:16 PM

@Dob: Mint itself may be read-only, but they deliberately gloss over the fact that, if their system were compromised, attackers could get your bank credentials. An attacker with access to your bank credentials can do anything that your banks allows you to do online

I think it's far past time that banks start having multiple privilege levels. Corporations get this sort of treatment, but we the lay-person do not. I'd like to see the ability of x person to pay known billers, for example, or a read-only version. For all the technology available to us, banks in this country are truly still in the stone age, service wise.

Posted by: Chris at May 23, 2011 2:46 PM

@Glenn Fleishman

"I scrupulously avoided accusing Dropbox of lying, because the record makes it clear..."

Nice work. Agreed.

Hey, I love to make snarky complaints about cloud security as much as anyone but calling Dropbox a liar is a stretch.

Dropbox has been quick to respond, clarify and explain themselves; they have not changed their services, only clarified what was unclear.

The logic of the complaint that was filed with the FTC doesn't pass even the most basic tests. There's no foundation for their "best practices" claim, for example, as I explained in far too much detail here.

http://www.flyingpenguin.com/?p=11934

More to the point, the recent NIST cloud security announcement totally contradicts their complaint.

http://www.flyingpenguin.com/?p=11988

NIST SP 800-146 DRAFT Cloud Computing Synopsis and Recommendations

"It is an open issue on how to use cryptography safely from inside a cloud. "

Posted by: Davi Ottenheimer at May 23, 2011 3:41 PM

Any incremental/differential/delta backups leak metadata to the storage provider. For instance you download a particular delta then they know the time period of the file version you want. If you read the start of a backup followed by a later extract they can guess the size of the index portion which shows roughly how many files you have.

If you believe properly encrypted data is that where without the key you cannot tell it from random data then I think these guidelines follow: Use only full backups. Use only full restores. There is no verification mode short of a full restore.

Verification should be made onto different hardware then the original. If you're an organisation then verification should be done by different people.

Posted by: 087024111 at May 23, 2011 4:14 PM

All of you claiming that Dropbox lied are assuming intent. What motive would they have? Are far more likely explanation is a mistake. The terms of service were never deceptive. The complaint is about the help page, probably written by some poor tech writer.

A mistake was made and corrected. Move on.

Posted by: Logan at May 23, 2011 4:56 PM

Offtopic story proposal:

"Crazy Military Tracking Tech, From Super Scents to Quantum Dots"

http://www.wired.com/dangerroom/2011/05/...

Posted by: H at May 23, 2011 5:36 PM

@ Davi Ottenheimer

I concur with your analysis. Whether or not they lied or to which extent they are getting their crypto right is not even the main issue. What I fail to understand is how anyone in his/her right mind can believe that any profit based organisation will:

- Provide a free service
- Not collect any personal information
- Get confidentiality, integrity and availability controls right
- Give a toss about the privacy of your data when subpoenad over them
- Inform you correctly when your data and/or their infrastructure has been compromised.

The entire concept is just plain ludicrous. If you want your data to live safely in the cloud, it's really up to yourself to secure them before moving them there.

@ Logan

I'm afraid that's just too naieve.

Posted by: Dirk Praet at May 23, 2011 6:12 PM

@"Clive"
There realy is not space to list even a few of them (not without upsetting the other readers).

Who are you and what have you done with the real Clive?

If it's one thing readers of this blog have come to expect it's long, thought-provoking posts (with the odd typo) from the real Clive!

http://www.schneier.com/blog/archives/2010/03/...

Posted by: Thomas at May 23, 2011 6:39 PM

I have to agree wit Dirk: any data not under your direct control is not secure (for sure - and data under your direct control probably isn't, either). This follows from my "there is no security" meme.

On the other hand, there is a matter of degree. If you want to keep your porn collection reasonably secure from your wife or your boss, my guess is that Dropbox's level of security is fine.

If you're bin Laden - oh, wait, he's (supposed) to be dead - then it's not adequate.

There's "security from the riffraff" and "real security". The former is more or less possible, the latter a fiction.

I just was reading yesterday about the "Bling Ring", the burglars who robbed Paris Hilton's house in LA an ungodly number of times, as well as numerous other celebrities. An amazing number of those people had fences (cut through), security cameras (the burglars didn't even wear masks, just hoodies), and safes (left open), and the burglars basically just tried doors until they found an unlocked one (they almost always did).

With such a degree of security, it explains why celebrities need to make so much money - they need it to replace all the stuff so easily looted by incompetent teenagers.

Imagine what could happen if professional burglars decided to hit celebrities instead of "riff-raff".

Posted by: Richard Steven Hack at May 23, 2011 7:53 PM

Thomas: "long, thought-provoking posts (with the odd typo) from the real Clive!"

This is how Clive authenticates himself to his or any other systems. This is the only example I know of "real security"! :-)

Posted by: Richard Steven Hack at May 23, 2011 7:55 PM

@Shachar:

Why not use a tweakable block cipher, you know, like is used for encrypted hard disks? They certainly don't rewrite the whole drive to change a block at the start - there's modes other than ECB and CBC these days...

Or does your algorithm cope with non-block-length insertions and deletions?

Posted by: Jay at May 23, 2011 8:01 PM

Only slightly offtopic as it deals with crypto storage:

Self-Erasing Hard Drives Introduced by Toshiba
http://technorati.com/technology/gadgets/article/...

While these might be very useful for your average hacker who needs a way to clean his drive when the Feds break down the door, I can't wait for a bug to be discovered when someone's critical data gets erased "accidentally".

It's also not clear to me how long it takes these drives to actually wipe the data. If it takes as long as running external software to do so, then pulling the power probably stops the erase - which makes it worthless for hackers or anyone else who will be subject to someone capable of yanking the internal electronics and reading the platters anyway.

Still, I suppose for corporates or individuals concerned about their private data being exposed from a laptop theft, these might have their uses - as long as the thieves are "riff-raff" and not competent techs with the right equipment.

Posted by: Richard Steven Hack at May 23, 2011 8:42 PM

Many of us put blind faith into the security claims of Online services. Thanks for highlighting the potential issues with Dropbox and their competitors!

Posted by: Gary at May 23, 2011 9:27 PM

@Richard: "It's also not clear to me how long it takes these drives to actually wipe the data."

If it's set up the same way as other hardware-encryption drives, erasing the key is all that's needed. Once it's erased (let's say the magnetic bits with the key are rewritten with garbage 27 times or 100 or whatever, still in the space of seconds), the data is permanently irrecoverable unless the NSA or other governments have cracked current encryption systems that are seen as requiring millions of years to overcome.

Posted by: Glenn Fleishman at May 23, 2011 9:53 PM

@ Glenn Fleishman

That's over simplifying the issue. For one, we can't even be sure the software on the drive acts in the way you describe. Remember the government-certified USB stick that was compromised and reported on this blog? The user entered a password into the PC, the software sent an "open" signal, and the drive was unlocked. Just sending the "open" signal was all it took to defeat the "256-bit uncrackable encryption."

But, assuming they did do a correct high-level design, there's still the possibility of information leaks in the form of storage, timing and side channels. There might also be a potential attack on the RAM itself, although this requires more technical sophistication & has to be performed right after the device is used.

Anyone interested in self-destroying or high assurance crypto designs should google Clive Robinson and I's discussions on the subject on this blog. We worked out quite a lot of angles. Basic covert channels

and DMA are the main issues, assuming everything else is implemented correctly. There's a reason so many of those NSA-approved Type 1 encryption devices don't go past 80Mbps performance: one must sacrifice plenty to resist these sophisticated attacks. The mass market has always been unwilling to make these sacrifices, so I don't trust mass market products by default.

Posted by: Nick P at May 24, 2011 1:27 AM

@youlose "I lose deniability of TrueCrypt hidden volume ".

Its getting silly, but you could nest your truecrypt volume with deniable part inside a truecrypt volume you sync with dropbox.

Posted by: hash1baby at May 24, 2011 3:31 AM

"Its getting silly, but you could nest your truecrypt volume with deniable part inside a truecrypt volume you sync with dropbox."

Yeah, pretty silly compared to... say... just not using dropbox.

Posted by: Nick P at May 24, 2011 3:48 AM

(I am biased as, on the whole I believe the cloud is an epic fail waiting to happen)

In this instance, I actually dont think Dropbox lied and I dont think they are any worse than any other cloud provider, so singling them out as if it is *them* at fault rather than the whole environment is a mistake.

As mentioned above, it is unrealistic to assume a profit-making company will provide a service for free without major compromises being in place.

If you want to be able to sync files on your iPhone, iPad and desktop PC there is a temptation to use dropbox (and truecrypt is out) but you have to accept the fact you are basically sending these by postcard. For most home users this is an acceptable trade-off for the ease by which they can move pictures of their naked partner *but* the problem is people are not aware of the risk they are accepting.

This is my biggest issue with Cloud (and dropbox) - in that users are given a fairly hard sell on the benefits but are kept in the dark about the risks they are accepting. You can say its down to the individual to research their risks before they sign up, but that is unfair and realistically most people wont.

I work at a company where executives have iPads and I know for a fact they are moving official information back and forth to these devices. I cant imagine they are doing it in any way other than using Dropbox.

There is an assumption, because of some basic use of authentication credentials, that the data being sent is private and safe.

Until cloud service providers are forced to have warning notices, my efforts to raise awareness hit up against the marketing machine that says "everything about the cloud is great, stop asking questions."

Posted by: GreenSquirrel at May 24, 2011 4:11 AM

@Zach

Truecrypt uses XTS block mode: it means that the software encypts just the cipher blocks that have changed. Obviously, it leaks out informations about the extent of the modification/update but for me that's not a big issue.

@youlose

The paper you're referring to is about defeating the plausible deniability feature of truecrypt, not the encryption itself. They show that perfect plausible deniability isn't possibile due to leaked infos by the inner OS during normal execution. What's the deal with my solution?

Posted by: Gianluca Ghettini at May 24, 2011 5:15 AM

@vedaal

ops, sorry... my fault! Actually, Truecypt does *not* generate password for u. Instead, I was thinking about KeepassX, a great open source tool that I use on a regular basis to securely store all my accounts/passwords.

Posted by: Gianluca Ghettini at May 24, 2011 5:24 AM

Hi, I'm the developer of SecretSync, http://getsecretsync.com a client-side encryption tool for Dropbox and other sync tools. We built SecretSync largely due to (1) our desire to take advantage of the cloud, specifically Dropbox, and (2) our fear of trusting unknown people and servers wholly with our data.

@BF Skinner: "If you're not doing anything wrong what do you have to hide?"

This statement is bit too glib for my taste. I'm doing nothing wrong, and there are certainly things I want to hide. My finances, will and testament, source code, perhaps some nostalgia like letters, etc. I personally use Dropbox (via SecretSync, so encrypted) as an offsite backup for my Quickbooks and GnuCash files. I don't want to lose that data, say in a fire, but I also don't want anyone to know my business. Nothing criminal, just private.

@GreenSquirrel: "In this instance, I actually dont think Dropbox lied and I dont think they are any worse than any other cloud provider... my biggest issue with Cloud (and dropbox) - in that users are given a fairly hard sell on the benefits but are kept in the dark about the risks they are accepting."

I think Dropbox is getting the brunt of what is a problem in the paradigm. With the cloud, everything is physically controlled by someone else. Do you know these people personally? Have you had a chance to assess they're honesty and competence? Probably not. So you have to take a few documents on there website, i.e. terms of service, security page, as truth, and accept the risks.

Naturally, their marketing department is going to downplay the risks and only talk about the benefits: You don't have to maintain servers, worry about upgrades, it all works in the browser, etc. But all convenience comes at some cost.

Posted by: James A. at May 24, 2011 9:29 AM

"... need for privacy -- most often because they are breaking either a just or unjust law -- need..."

I love that he tries to make it sound more reasonable by slipping in "just or unjust". Basically, "I'm not saying they're *bad* criminals... I'm just saying that only criminals need privacy"

Posted by: Q at May 24, 2011 10:15 AM

@ James A,

"@BF Skinner: "If you're not doing..."

I'm guessing you are fairly new to this blog.

Most long term blog readers/posters here tend to treat the phrase as an intro to a joke etc much like you would use "Have you heard the one about..." if you read BF Skiners comment a couple of lines down (ie why American's don't go without clothes) you will see it was ment as sarcasm etc to my earlier comment.

P.S. after a while here you will see occasionaly we are sort of "rude" to each other here (BF Skinner thinks I might be a Klingon etc 8^)

Posted by: Clive Robinson at May 24, 2011 10:38 AM

Seems to me that loudly and ostentatiously announcing that there are vulnerabilities but that they're going to remain secret strongly resembles the "whooooooosh" a fly fishing reel makes as the lure and baited hook go flying through the air. Someone's either interested in recruiting new blood, or harvesting low hanging fruit. :)

Posted by: Trichinosis USA at May 24, 2011 11:31 AM

"P.S. after a while here you will see occasionaly we are sort of "rude" to each other here (BF Skinner thinks I might be a Klingon etc 8^)"

And I called him British... :P

Posted by: Nick P at May 24, 2011 3:17 PM

@Clive Robinson, noted, and thanks for the gentle treatment. :)

Posted by: James A at May 24, 2011 4:34 PM

Although many tech-savvy users must have known that Dropbox has to have access to our files (for features like the web interface), the regular "mainstream" user does not have the knowledge to assume this fact. That's why Dropbox should have communicated this issue much more to the public then just answering to a few questions in their forums.

There was always a trade-off between security and comfort and the success of Dropbox shows clearly what the majority of users prefers: the later. The opposite and very small group of users create their own custom rsync-over-ssl-over-vpn-over-xyz solution. And for users in between exist other services like Spideroak with built-in encryption or products like my file-by-file encryption tool BoxCryptor (http://www.boxcryptor.com) or PrivateFiles's SecretSync try to provide an additional privacy layer on top of non-trustable services like Dropbox.

It is important that a service is honest with its users about its data privacy and security policies so that

every user can make a solid decision which service to choose based on his preferences (comfort vs. security)

Posted by: Robert Freudenreich at May 24, 2011 5:50 PM

That's great advice, but it's not that simple. Many people use dropbox because their iOS device apps can get to it and access the data there, but those apps would not be able to decrypt it without having to support every third party encryption out there.

However, if Dropbox was like CrashPlan, and let you specify a private key to encrypt/decrypt your data, so that they can store it but they can NOT have access to view the contents, then you could enter the key into any apps supporting Dropbox and this encryption mechanism automatically as part of Dropbox support.

Posted by: Scott at May 25, 2011 12:03 AM

@Scott

I don't want to be rude but I think you're missing the whole point of cryptograpy. Any encryption system manged directly by Dropbox would be USELESS because it would NOT in your control so you could NOT trust it. The ecryption must be implemented on top of Dropbox by the user which owns the key (of course) and the encryption/decryption processes.

Posted by: Gianluca Ghettini at May 25, 2011 3:00 AM

@Glenn Fleischmann: "I'd love a file-by-file on-the-fly encryption system, myself."

EncFs does this: http://en.wikipedia.org/wiki/Encfs
I hear that it even has some sort of Windows port/fork/version.

Posted by: Paeniteo at May 25, 2011 3:57 AM

Not a single mention of Wuala as an alternative to Dropbox?

Posted by: Ingo at May 25, 2011 2:59 PM

I quickly realized that backing up an EncFS or eCryptfs tree means you can't exclude any unnecessary files unless you don't encrypt the filenames. I tried to back up an encrypted home folder to an online backup service and ran out of space (as well as transferred a lot of useless data) because there was no way to know or specify which encrypted subfolder names to exclude. Firefox/Chrome/Google Earth etc. all store their cache somewhere in the home folder. Ubuntu, at least, appears to have a general user .cache folder that applications can put subfolders in, but even then, you can't exclude .cache when it's been named something random.

So now I'm trying to find some other software I can use in combination with rsync to re-encrypt the decrypted versions of the data before upload. Supposedly CrashPlan would be acceptable if I controlled the other end, assuming I trust their software. It'll probably have to be something like duplicity. I've spent tens of hours researching and have yet to settle on an acceptable solution. Even for something that looks good, I've read that either verifiable restores are a chore or restores are unreliable.

Posted by: Nick S. at May 25, 2011 3:22 PM

@ Gianluca Ghettini

Actually, that's not the whole point of cryptography. Cryptography is a security primitive for enforcing a security policy. Different users have different policies/requirements. Many users don't care if Dropbox can read their stuff, but don't want others to read it. For instance, a company might host internal memo's on a cloud storage provider and trust the provider not to give the information to the competition.

Any time that the user wants entities other than the service provider to be denied access, then using cryptography to protect data in transit to the service provider is a viable option. I don't think it's the best option. I prefer protocols like those you describe. But this is another case of user priorities deciding on a provider for reasons other than security. Dropbox is mainly picked for ease of use, cross-platform capability, and the free storage. They shouldn't have lied about their security profile, but had they told the truth most of their customers would still have used them.

Posted by: Nick P at May 25, 2011 3:52 PM

What about cloud based electronic / digital signature services where they generate and store online the keys used to digitally sign documents uploaded by their users (documents which are also stored online) which are also shared with other parties online through the same cloud service? See www.docusign.com.

Can non-repudiation really apply in such a case?

Posted by: Tsaixingwei at May 25, 2011 6:02 PM

@ Tsaixingwei

That sounds pretty weak for non-repudiation. A private key could be stored anywhere so long as it's encrypted. However, if they have it in plaintext, we can't be sure who signed the document. A better cloud model might be a Java applet or JavaScript site that retrieves the encrypted private key, decrypts it via user-supplied password, signs a file, and uploads the file and signature to the service provider. This allows things to be web based and keeps the actual signing key out of the hands of service providers.

Of course, it brings with it all the usual headaches of cloud- or browser-based crypto. I don't think the cloud has a place for directly protecting secrets or doing non-repudiation besides maybe timestamping or acting as a digital notary. There are some very trustworthy services that do these things. Confidentiality goals, though, don't really fit with web browsers and the cloud model.

Posted by: Nick P at May 25, 2011 6:25 PM

@ Nick P

Let see the two scenarios:

Encrpytion (managed by user) -> then -> Dropbox
In this case, user leverages confidentiality and authentication (only the user with the right key can access and see plain data)

Dropbox -> then -> Encryption (managed by dropbox)
In this case user leverages nothing. Confidentiality and authetication come only if dropbox is a trusted thirty party.

That's the problem of all cloud-based service.

The point is that if the user has to trust the service in the first place then every encryption system implemented down the chain is completely useless.

Posted by: Gianluca Ghettini at May 26, 2011 4:15 AM

It actually sounds as if, rather than lying, Dropbox suffers from a very common problem at tech companies: the marketroids don't talk to the technical side of the house, don't have any significant understanding of how the product works, and don't believe it even matters.

Whenever asked in technical forums, they admitted they had access. All the claims of not having access, come from marketing literature.

Posted by: Roger at May 30, 2011 9:25 AM

I've had a Pro account at Dropbox for two plus years. I don't know as much about file encryption as I should but to be honest I never thought my Dropbox files were encrypted since I never had to create a key- nor did I receive an auto-generated key as I did with my Amazon S3 account. What does bother me though is the untrue wording that was on their Help page along with several posts they made in their forum stating the same untrue info. I especially didn't appreciate their April 21 blog post in which they tried to brush over all the apparent problems as misunderstandings because they "…have to communicate with people both familiar and unfamiliar with the intricacies of encryption and online security." So Dropbox feels that they must communicate in terms that explains their security in a way that the most ignorant of users will hopefully understand all those complex concepts? Not a valid reason for the obvious falsehoods and omissions.

I make it a point to place only non-secure, non-critical files in my Dropbox. Guess it's time I finally learn about encrypting my own data, huh? And I think I will go ahead and take a hard look at SpiderOak or Wuala for my online file storage. I just don't like the reasons Dropbox gives for their transgressions.

Thank you.

Jim McGowan

Posted by: Jim McGowan at May 30, 2011 1:55 PM

The moral of the story is that the DropBox folks lied to everybody, hoping to suck in a big user population (Facebook anybody?) Of course, DropBox (and its lookalike friends) will be the next target of the recording and movie industry associations, with almost absolute proof in hand that you are a violator (look, it's YOUR userid and password and you performed these actions with our copyrighted files, now PAY UP and/or go to jail!) No need for lawsuits, just call homeland security (the association police) and they will take care of everything. And ebooks will be right there with audio and video files as well as electronic news and other content. And don't even think about posting any web links (URLs) in the shared DropBox area as many web based entities now consider that to be a copyright violation and unlicensed/unauthorized usage. You thought these tools were for your ease of use and convenience?

By the way, it is clear that the shared storage area is on some server farm controlled by DropBox. How long before they invoke the "all your data are belong to us" rule...oh, wait, that is already the case since

they are reading and changing your files, with nothing to stop them from using your files and content (their terms of service is to control you, not them; remember Google desktop). Further, it is not beyond the realm of imagination that they already do have access, or will make use of access, to your computer for purposes above and beyond just sharing the files you have "given" to them. Others have also attempted "all your computer are belong to us" as well. Is DropBox just a more socially acceptable form of spyware?

Posted by: kashmarek at June 2, 2011 6:21 AM

If you need to send files to someone in the most secure way then 1. encrypt them if storing on the cloud. 2. deploy your own infrastructure [FTP, web server] where you can control everything or 3. use specialized software like Binfer [http://www.binfer.com] that does direct computer to computer encrypted transfers without uploading files anywhere.

Posted by: Daniel at October 24, 2011 9:07 AM

Subscribe to comments on this entry

Post a comment

Name:

Email Address:

E-mail is optional and will not be displayed on the site.

URL:

Remember Me? Yes No

Comments:

Allowed HTML: <a href="URL"> • <cite> <i> • <b> • <sub> <sup> •   • <blockquote> <pre>

Preview **Post**

Powered by Movable Type. Photo at top by Geoffrey Stone.
