

Re: Usenet Fuckology-101

Source: <http://sci.tech-archive.net/Archive/sci.space.policy/2007-05/msg00528.html>

- *From:* BradGuth <bradguth@xxxxxxxxxx>
 - *Date:* 26 May 2007 14:16:24 -0700
-

On May 26, 12:46 pm, "Jonathan" <w...@xxxxxxxxxxxxxxxx> wrote:

"BradGuth" <bradg...@xxxxxxxxxx> wrote in message

news:1180190283.105168.245900@xx

When I get my multi terabyte PC or MAC, I too would be interested in having the likes of Xnews at my disposal. However, that's still not related to what the public is getting to see.

Usenet as such should be for the greater public good, and not for the greater evil, as it currently is.

The local ISP and of whatever's GOOGLE served are each capable of knowing where each and every byte is going, and of where each byte originated. Their computers know of this because, without such knowledge is where all that's internet or usenet would soon enough fail to function. Ignoring and thereby allowing whatever is known as being bad for us as end-user clients, is exactly what the likes of Hitler or worse cults would do, and it's also why we'd long ago started taking advantage of, poking fun at and of why we're still at war with those mostly innocent Muslims, along with active plans for an all out WWII of global energy domination if necessary against primarily other Muslims.

OK, well if you're paranoid about govt snooping, here's a faq designed to thoroughly frustrate any and all govt agencies from bothering you online. It is possible to send messages to usenet with complete

anonymity even from the most capable agencies.
Keep the text, as links to this faq
have a way of disappearing.

Having the ability to post anonymously is a basic
human right, and the path to maintaining a free
and open internet that will serve the rights of
the people, instead of restricting them.

This version of the faq is a bit dated and some
of the links may not work anymore. But this
is the security faq from the ng that caused
the NSA to write the carnivore program, which
can word search any e-mail. The security
faq was that good. Once the govt agencies
realized they couldn't silence any dedicated
speaker, they decided on another path.
To ban all adult speech on the internet
with the Communications Decency Act.
That law passed but led to a Supreme Court
challenge that gave the internet First Amendment
protection in Reno v ACLU.

-----BEGIN PGP SIGNED MESSAGE-----

Security and Encryption FAQ Revision 15

by

"No one shall be subjected to arbitrary interference with his privacy,
family, home or correspondence, nor to attacks upon his honour and
reputation. Everyone has the right to the protection of the law against
such interference or attacks."

Article 12 Universal Declaration of Human Rights

Disclaimer and justification for this FAQ.

Many countries operate a legal system designed to suppress individual
freedom. Such countries often do not obey basic human rights. The law
in these countries may be based on guilty until proven innocent. My
intention in offering this FAQ, is to legally challenge these threats to
our freedom. It is not my intention to promote any illegal act, but to offer
people the option of freedom of choice. How they use that freedom
is entirely down to the individual.

Revisions in this version of the FAQ include BestCrypt version 6. BestCrypt
has been included because the latest version 6 has a particularly useful
undocumented feature that offers a form of plausible deniability that is all
but undefeatable, so far as I know. More about this later in the FAQ.

Re: Usenet Fuckology-101

The FAQ has 2 main Sections.

Part 1 concentrates on passive security. It is intended to be useful to both posters and lurkers.

Part 2 is to maximize your privacy whilst online, particularly for Email and Usenet posting.

I have assumed three security levels:

Level 1. For those who wish to protect their files from unauthorized access. These users are not too concerned at being found with encrypted data on their computer.

Level 2. This is for those who not only wish to hide their private data, but to hide the fact that they have such data. This might be an essential requirement for anyone who lives in an inquisitorial police state where human rights are dubious, or where there is no equivalent to the United States 5th Amendment.

Level 3. This is for those who not only need all that is offered by level 2, but additionally wish to protect their computer from unauthorized access. Protecting themselves from hackers whilst online and snoopers who may try and compromise either their software or add substitute software that could reveal their secret passphrases.

Part 1 explains the 3 security levels and offers help in achieving them.

1. How does encryption work?

In its simplest sense, the plaintext is combined with a mathematical algorithm (a set of rules for processing data) such that the original text cannot be deduced from the output file, hence the data is now in encrypted form. To enable the process to be secure, a key (called the passphrase) is combined with this algorithm. Obviously the process must be reversible, but only with the aid of the correct key. Without the key, the process should be extremely difficult. The mathematics of the encryption should be openly available for peer review. At first sight this may appear to compromise the encryption, but this is far from the case. Peer review ensures that there are no "back doors" or crypto weaknesses within the program. Although the algorithm is understood, it is the combination of its use with the passphrase that ensures secrecy. Thus the passphrase is critical to the security of the data.

2. I want my Hard Drive and my Email to be secure, how can I achieve this?

You need Pretty Good Privacy (PGP) for your Email and either Scramdisk or BestCrypt for your private files on your computer.

PGP is here:<http://members.tripod.com/cyberkt/>

Scramdisk is here:<http://www.scramdisk.clara.net/>

BestCrypt is here:<http://www.jetico.com/>

Both PGP and Scramdisk version 3.01R3c are free. The newer version of Scramdisk, version 3.02A is not free. BestCrypt is commercial ware. The source code has been published for PGP and for Scramdisk version 3.01R3c. The source code for version 3.02A has not yet been published. The source code for the encryption side of BestCrypt has been published, but not the proprietary Windows interface. Scramdisk version 3.02A, BestCrypt and PGP support Win95/98/2000 and NT.

3. What is the difference between these Programs?

PGP uses a system of encryption called public key cryptography. Two different keys are used. One key is secret and the other is made public. Anybody sending you mail simply encrypts their message to you with your public key. They can get this key either directly from you or from a public key server. It is analogous to someone sending you a box and a self locking padlock for you to send them secret papers. Only they have the key to open the box.

The public key is obviously not secret – in fact it should be spread far and wide so that anybody can find it if they wish to send you encrypted Email. The easiest way to ensure this, is by submitting it to a public key server.

The only way to decrypt this incoming message is with your secret key. It is impossible to decrypt using the same key as was used to encrypt the message, your public key. Thus it is called asymmetrical encryption. It is a one way system of encryption, requiring the corresponding (secret) key to decrypt. PGP is simplicity itself to install and use. I recommend you use one of the Cyber-Knights versions.

For your normal hard drive encryption, you will need a symmetrical type of encryption program. The same key is used for both encryption and decryption. Scramdisk and BestCrypt are especially good because they are "On-The-Fly" (OTF) programs. This means that the program will only decrypt on an as needed basis into RAM memory. More about this later in the FAQ.

One question often asked by newbies is whether the passphrase is stored somewhere within the encrypted file. No. The passphrase is passed through a hash, such as SHA1. This is a one-way encryption. This output hash is what is stored within the encrypted container. The program will look for this hash and compare it with the hash it produces from the passphrase that you type in to mount the container. If they are identical, the container will be decipherable and will be mounted.

4. I have Windows 95/98, am I safe?

Re: Usenet Fuckology-101

Windows is definitely not a security orientated program. One simple method of improving your computer security is to disable the Windows swapfile. To ensure reliable operation and dependant on what programs you run, you may need several hundred megabytes of RAM. If you are serious about your privacy, I would recommend investing in as much RAM as you can afford and turn off the swapfile. I suggest a minimum of 128 Megs and preferably double or even quadruple that.

5. Apart from the Swapfile, what else can Windows reveal to a snooper?

User.dat can reveal all sorts of interesting things about your computer habits. Take a peek by opening in Notepad or Wordpad. Press CTRL-F (i.e. the Control key and the F key together). Type in the box, X:\ (or whatever drive letter you use to store any critical data). Press "Find" and continue throughout the file. Alternatively, you could input .jpg, or .avi, etc – you get the idea. You cannot edit this file in Notepad or Wordpad. The only way to edit user.dat is by using regedit.exe. My experience suggests you will not be able to easily remove embarrassing entries.

If you find information that you would rather not be there, you will either need to restore from an earlier backup of these files, or simply bite on the bullet and re-format your hard drive. This is extreme, but may be the only alternative. At least you then start with a clean slate.

Remember the format command: Format c: /s (it is vitally important that you include the /s to install the system files). Obviously back up your data, Email address book, etc., etc., before proceeding.

Dependant on how paranoid you are, after formatting you may choose to first install "Zapempty" or another Dos based

read more »– Hide quoted text –

– Show quoted text –...

Thanks once again, for what I pretty much already knew about.

I'm actually hoping that whatever MIB or government spooks keep doing their usual topic/author tactic of stalking, bashings and banishments, as well as their efforts of contributing their silly spermware/fuckware that's clearly intended for terminating my poor old PC, as that only proves I'm worth the effort.

Keeping my message(s) up for the public to review without custom encryption, seems the only right thing to be doing. Unlike yourself and most others in Usenet, I'm not trying to hide. Unfortunately, my home is within friendly fire range of various local DoD training, so I'm hoping that such mainstream damage-control will not go quite that far.

–

Brad Guth