

Discussion – Protecting Your Privacy

Introduction

In the wake of Edward Snowden's leaks about the American PRISM project which hoovers up all the data it can from all the internet traffic which it can access it is, perhaps, relevant to look at ways to prevent snooping on your emails. You can make your emails private using a process called *encryption* but this is more than most people are prepared to do.

The other part of the internet, your internet browsing and searching, is something which you cannot keep private because everything on the internet is sent in the clear. This means that you cannot encrypt your internet traffic because the internet is designed so that anybody can read anything on the internet.

However, there is a system of routers (known as TOR) which encrypt the traffic while it is within the system of routers but, as with all other internet traffic, your traffic is unencrypted once it leaves the TOR system.

TOR

There is no way to stop anybody from checking your internet dealings if they have access to all the traffic which flows through your ISP's connections. There is an interesting product, TOR (which stands for The Onion Router), which everybody can use to make their browsing anonymous. Unfortunately, because TOR makes your internet traffic anonymous, those who are in the business of finding out all they can about you will be watching the TOR traffic.

If you are connecting with another party which encrypts its internet traffic, and you know the encryption key, your traffic can be both anonymous and private. This is a great way for those who want to pass information anonymously (perhaps as a whistle blower) to keep their identity secret and ensure that their information is delivered securely.

Steganography

If you send an encrypted email anybody who has access to your internet traffic can tell that an email has been sent. They may not be able to read the contents, but the fact that an email has been sent from your computer to another person is known. This will allow the bad guys to work out the connection between you and then try other means to work out what you are sending to each other.

Steganography, on the other hand, hides your message in another medium so that only you and your partner in crime know that there is a message. There are many ways to achieve this, but perhaps the best known is the use of images to hide the message. Steganography, from two Greek words meaning "secret writing", when used with images to hide the message, usually changes one or two bits of some of the pixels in an image. The shorter the message and the larger the image the less chance there is that a snooper would be able to determine from a quick look that the image had been tampered with.

The primary aims of steganography are to hide the fact that a message is hidden in another medium and to hide the contents of the message. If the presence of a hidden message is suspected then the person who is looking for the hidden message will try all sorts of attacks to find the contents of that message. There are a number of tools around that will hide a message in an image, a sound file or a movie. There are also a number of tools around which can look for the signature of the encryption tools in a message so the best chance of having your message delivered unchecked is to ensure that the existence of the hidden message is not suspected.

Email Encryption

If you need to have private communications with a friend or work colleague then you need to encrypt your emails. This usually means installing a program like PGP (Pretty Good Privacy) then getting their public keys from all the people who we will want to contact. This can be a pain!

A company called Firetrust is developing a program called EncryptUs which, when finished, promises to remove all the hassles from email encryption. This company is the one which makes one of my favourite programs: MailWasher. If you go to the EncryptUs website you can be sent emails from the development team. Hopefully, this will encourage them to finish this product more quickly!

Cloud Data Storage

Everybody seems to have heard about cloud storage, but many are not sure just what cloud storage is. The main point of cloud storage is that your data is stored on a computer outside your control. This, for me, is the best reason to be wary about using cloud storage. If you do plan to use cloud storage then please encrypt your data with a strong password.

The reason for this is simple. The companies that provide cloud storage are mostly American and the NSA (National Security Agency, the most secretive of the American secret agencies) has ways of making them cooperate and allow access to your data. If your data is encrypted with a strong password then you have more chance of keeping it safe from prying eyes and computers.

Creating Safe Passwords

It is easy to create a safe password, and the mathematics are easy. For those of you who do not like thinking about mathematics then the rules for creating a safe password are easy:

- Ensure that you have at least one uppercase letter (ie A, B, C, ... Z)
- Ensure that you have at least one lowercase letter (ie a, b, c, ... z)
- Ensure that you have at least one digit (ie 0 ... 9)
- Ensure that you have at least one special character. Special characters are those which are created by holding shift and pressing a number key. There are others like {, }, [,], \, |, ` , ~, :, ;, “, ‘, /, ?, < and > as well as a comma and full stop. This give a grand total of 32 special characters.
- Finally make sure that you a number of repeated characters to round out your password.

For example: my name is Toby so my password could be Tob! plus six @ signs making the final result Tob!@@@@@.

The Mathematics

The mathematics are easy. There are 26 uppercase letter, 26 lowercase letters, ten digits and 32 special characters. By using one of each you are forcing the attacker to check 94 (26 + 26 + 32 + 10) possible entries in each of the ten positions of the password. And, to make matters more difficult for the attacker, the password must be an exact match and he or she or it does not know the length of your password.

Now, from your school days, you will remember that if you have one digit it can contain any number from 0 to 9. This is a range of 10. If you have two digits it can contain any number from 00 to 99, which is a range of 10 x 10 (= 100) or 10². Add another column and you increase the possible range by a factor of ten to 10 x 10 x 10 (= 1,000) or 10³.

Now, if you use a larger number of possible entries in each position, you rapidly increase the number of combinations of characters which have to be tried. If you use one uppercase letter,

one lowercase letter, one special character and one digit, you have to try each of 94 possible entries in each of the positions of the password. 94^{10} works out to more than 5 followed by nineteen zeroes! This reads as 50,000,000,000,000,000,000: and that is the number of possible attempts your attacker has to try. Now, if you add just one more @ then you have made your attacker's job nearly 100 times as difficult!

And the best part is that you only have to remember four characters and the number of times that the fifth character repeats! Easy for you; difficult for your attacker!

Further Information

TOR www.torproject.org