

How to take back you privacy?

Naam, Genma

EPITA / Gconfs
naam@riseup.net
genma@riseup.net

01/17/13

Overview

1 Intro

- Why we do this talk ?
- The digital identity
- Questions ?

2 HOW TO : Encryption

- WTF is encryption ?
- What can I encrypt ? How ?
- Questions ?

3 HOW TO : Anonymity

- Why does it matter ?
- There is always a tool that fit your need
- Questions ?

4 Conclusion

- We're not in a XOXO word
- Cryptoparty
- Questions ?

Sensitive data

Definition

- a set of values of qualitative or quantitative variables
- individual pieces of information

Some of them are (important|critical)s, don't play with Mallory.

The right to stay anonymous

The Convention for the Protection of Human Rights and Fundamental Freedoms states that :

Article 8 - Right to respect for private and family life

- Everyone has the right to respect for his private and family life (...).
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society *in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

You will also see

- Tons of softwares, distributions, techniques to defeat too inquisitive people and censorship.
- What's a Cryptoparty and what you could learn from it.



About me

Where can you find me on Internet ?

- Blog (in French) :
<http://genma.free.fr>
- Twitter :
<http://twitter.com/genma>

My Hobbies ? Many things

- Crypto
- Privacy



Digital identity, what is it ?

Definition

- Digital identity is all the public data you can find about someone using Internet research.
- It's the famous e-reputation.

What do you think of me?

Google you name

- The results shown are they exactly what you want ?

[Le Blog de Genma ...](#)

genma.free.fr/ ▼

Interview de Skhaen, Telecomix et Cyphercat.eu. publié le 13 septembre 2013 par **Genma**.
C'est via sa conférence à PSES2012, traitant de la cryptographie et ...

[Genma \(genma\) on Twitter](#)

<https://twitter.com/genma> ▼

The latest from **Genma** (@genma). **Genma** - Compte Officiel ;-) - Un peu linuxien, un peu otaku mais surtout Geek et Blogueur sur Le Blog de **Genma**. Paris.

[Genma Kun - France | LinkedIn](#)

fr.linkedin.com/in/genma ▼

Région de Paris , France - Geek, Blogueur, Développeur, Lifehacker
Voir le profil professionnel de **Genma Kun** (France) sur LinkedIn. Grâce à LinkedIn, le plus grand réseau professionnel au monde, les professionnels comme ...

[Genma Kun | Facebook](#)

<https://www.facebook.com/genma> ▼

Genma Kun is on Facebook. Join Facebook to connect with **Genma Kun** and others you may know. Facebook gives people the power to share and makes the ...

Saying

Words fly, writings remain

- This adage is especially true with the Internet.
- It must be assumed that what is said will always be accessible, even years later.
- Everything on the Internet is public or will be (even if it is "private", Terms of Use may change).
- It is therefore not abuse the freedom of expression and remain respectful of laws.

Pseudonymity

Defintion

- Contraction of anonymity and pseudonym words, the term pseudonymity reflects quite well the contradictory of **being a public figure and to remain anonymous ...**
- Have a pseudonym does not mean to say and do anything.
- This is the image that I return, this is my credibility (past, present and future).
- A pseudonym is also a public identity, which is associated with different account : my blog, my Twitter, my Facebook account.
- The digital identity are all these public data associated with this identity.

Samples

Twitter



Linkedin



Genma Kun

Geek, Blogueur, Développeur J2EE/.NET, Lifehacker
Région de Paris , France | Internet

Pseudonymity is disappearing...

Facebook

- Facebook doesn't allow an account with a pseudonym.
- O RLY ? Look [http://www.facebook.com/genma;-\)](http://www.facebook.com/genma;-))
- The goal is to force people to express themselves using their real names,

Pseudonymity is seen as a problem

The problem is that the anonymity is take as an excuse to condemn the use of the Internet as a tool for freedom of expression.

If people are monitored, they do not say what they think, they do not criticize the politicians.

With the Internet, the citizen is gradually taking power on politicians.

Conclusion

Pseudonymity is a necessity

- Manage your digital identity.
- **Pseudonymity is the first step to take back you privacy.**

Something unclear ?



Feel free to ask for questions now.

Definition - cryptage, encrypt, encryption ?

Encryption

Encryption is to encrypt a document / file using an encryption key.
The reverse operation is decryption.

Cryptage

Term « cryptage » is derived from the English encryption and does not exist in French. Decryption is the fact of breaking the encryption when the private key is unknown.

Cryptography

Science is called Cryptography.

Encryption, how does it work ?

Symetric Encryption

This involves encrypting a message with the same key that will be used for decryption process.

Sample : Caesar code, with an offset letter. A->C, B->D etc.

Nous venons en paix -> Pqwu xgpqpu gp rckz

The reverse process is applied to get the message.

What is an encryption key ?

A key is called so because it opens / closes the padlock that is the used encryption algorithm.

- Here, the algorithm is the offset.
- The key is the number of offset of letter (here two letters).

Asymmetric Encryption 1/2

Public key - Private key

Asymmetric Encryption is based on the pair public key - private key.
⇒ What you need to know :

- My private key is... private and my own.
- My public key is shared with everyone.

The encryption algorithm

The encryption algorithm is more complex than the fact of shifting letters; it is based on mathematical concepts (first number ...)

Asymmetric Encryption 2/2

Encryption

With the public key of my correspondent, I encrypt a file.

⇒ The file can only be decrypted by the person who possesses the private key corresponding to the public key that I used (and therefore my correspondent).

Decryption

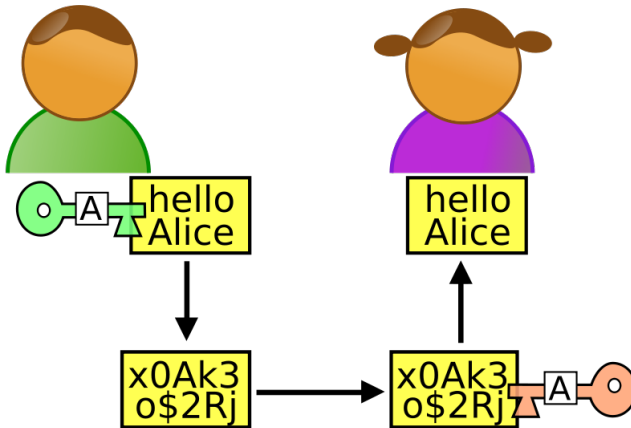
With its private key, my correspondent decrypts the file.

⇒ He can then read the message.

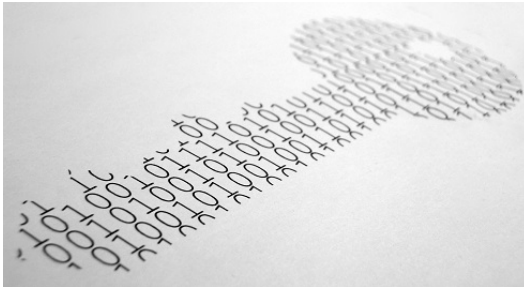
Concret case

Mail Encryption with PGP.

Bob send a message to Alice



Why encryption ?



Encrypt - The arguments against

Nobody does...

FALSE. Without knowing it, you do it every day.

Sample 1 : "padlock" when connecting (https)

Sample 2 : Wifi key.

Nothing to hide...

FALSE. Who would accept the postman read his medical post ?

Encryption, it's for the pedo-nazi...

FALSE. For journalists / bloggers dissidents who are denouncing dictatorships...

Encrypt - The arguments for

Encryption, it's not so complicated

It is not more complicated than using a "software". You just have to understand the principle.

Protection and security

My personal data are safe Cf. PRISM, NSA...

Privacy

Only the person for who the "message" is, is able to read it.

Edward Snowden

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.



Encryption limit

Which is encrypted can be decrypted today tomorrow

Tomorrow's computers will allow to decrypt the encrypted data today.

It the private key is lost

We no longer have access to data.

Metadata, social graph

PGP does not protect against the analysis of metadata (servers transit, addresses, headers, subject). Do not forget to clean the meta-data files (EXIF tag photos, office documents with tracked changes). DNS... Case of tracking Internet ...

Law and encryption

In France, the law therefore considers that the use of cryptology is free (LCEN Article 30-1) and there is therefore now no limit to the size of the encryption key that can be used .

In case of search, the refusal of submission of the encryption key may result in 3 years imprisonment and 45000€.

This penalty is increased if Encryption was used to commit a crime.

It is therefore recommended to give the decryption key, except in the case where the decrypted data would result in a judicial proceeding in which the final sentence would be greater than the interference with the judicial investigation.

Encryption

Locally - your data

- Hard disk
- USB Key
- Smartphone

Network - Communications

- Https : HTTPSEveryWhere for Firefox
- E-mails : GPG with Enigmail for Thunderbird
- Connexion : VPN, SSH, TOR...

⇒ Each "use", there is an encryption solution.

Emails - PGP, GPG ?

PGP

Pretty Good Privacy - PGP is an encryption software created by the American Phil Zimmermann in 1991.

OpenPGP

This standard describes the format of messages, signatures or certificates that can send software such as GNU Privacy Guard. It is therefore not a software but a format for the secure exchange of data, which owes its name to the historic program Pretty Good Privacy (PGP).

GnuPG

GnuPG (GNU Privacy Guard) is the free software.

Harddisk encryption

Software integrated in operating systems


- Windows 7/8 : Bitlocker (Backdoor)
- MacOS : FileVault
- GNU/Linux : Encfs...

Can you trust closed source software ?


Independently of the operating system

⇒ TrueCrypt. For a USB key/an external hard drive.

TrueCrypt audit


[browse](#) | [learn](#) | [create](#)

[Sign Up](#) | [Log In](#) |




The TrueCrypt Audit

People, businesses, and governments all over the world use TrueCrypt to protect their privacy. We need help making it better and more secure.


Technology – Research Triangle, North Carolina, United States

[Campaign Home](#) | [Updates / 0](#) | [Comments / 24](#) | [Fundors / 1166](#)



\$41,890 USD

Raised of \$25,000 Goal

 **29** days left

[CONTRIBUTE NOW ►](#)

Flexible Funding
 This campaign will receive all funds raised even if it does not reach its goal. Funding duration: October 14, 2013 - December 13, 2013 (11:59pm PT).

Share This Campaign: <http://igg.me/at/truecryptaudit/csbw> [★ Follow](#)

Select a Perk for your contribution

Encryption and privacy

Encryption is a need for privacy and allow data protection.

Something unclear ?



Feel free to ask for questions now.

Pseudonymity is disappearing...

Facebook

- Facebook doesn't allow an account with a pseudonym.
- O RLY ? Look [http://www.facebook.com/genma;-\)](http://www.facebook.com/genma;-))
- The goal is to force people to express themselves using their real names,

Pseudonymity is seen as a problem

The problem is that the anonymity is take as an excuse to condemn the use of the Internet as a tool for freedom of expression.

If people are monitored, they do not say what they think, they do not criticize the politicians.

With the Internet, the citizen is gradually taking power on politicians.

Conclusion

Pseudonymity is a necessity

- Manage your digital identity.
- **Pseudonymity is the first step to take back you privacy.**

TOR - The Onion Router

Présentation du réseau TOR

Tor est un logiciel libre,

- grâce auquel existe le réseau d'anonymisation Tor
- soutenu par l'organisation The Tor Project.

⇒ Techniquement, Tor nous permet de se connecter à des machines sur Internet via des relais.

⇒ Et cela de façon à ce qu'elles ne puissent pas identifier notre connexion (et donc de nous localiser).

A quoi sert TOR ?

Concrètement, ça sert pour :

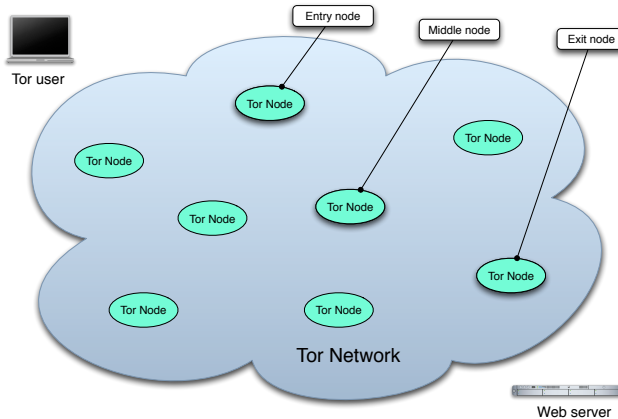
- échapper au fichage publicitaire,
- publier des informations sous un pseudonyme,
- accéder à des informations en laissant moins de traces,
- déjouer des dispositifs de filtrage (dans sa fac, en Chine ou en Iran...),
- communiquer en déjouant des dispositifs de surveillances,
- tester son pare-feu,
- ... et sûrement encore d'autres choses.

⇒ Tor dispose également d'un système de « services cachés » qui permet de fournir un service en cachant l'emplacement du serveur.

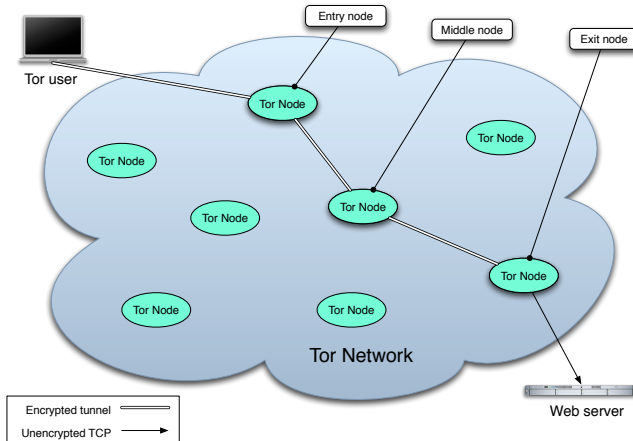
A quoi sert TOR ?

Tor est un réseau d'anonymisation, donc par définition, c'est difficile de faire un compte précis. Tor ne fait rien pour cacher que nous utilisons Tor. Donc quand en utilisant Tor, nous nous mettons au milieu de la foule des gens qui utilisent Tor. Plus cette foule est grande, meilleur est l'anonymat.

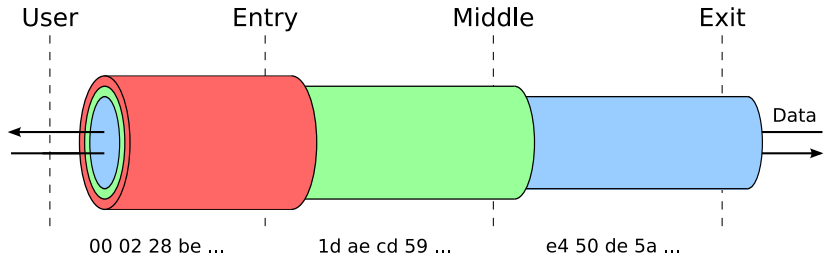
Comment fonctionne Tor ?



Comment fonctionne Tor ?



Comment fonctionne Tor ?



Comment fonctionne Tor ?

Ce tunnels se fait « en oignon » avec des couches de chiffrement empilées. Il y a une première clé de chiffrement vers le nœud d'entrée, une seconde clé vers le nœud du milieu et une dernière pour le nœud de sortie.

Il faut noter que Tor ne s'occupe pas de chiffrer après le nœud de sortie. Comme n'importe qui peut mettre en place un nœud de sortie, c'est une bonne idée de chiffrer sa communication en plus (par exemple en se connectant aux sites web que l'on visite en HTTPS). Après, se déroule tout un processus pour établir un tunnel chiffré jusqu'au nœud de sortie.

Utiliser Tor - Le Tor Browser

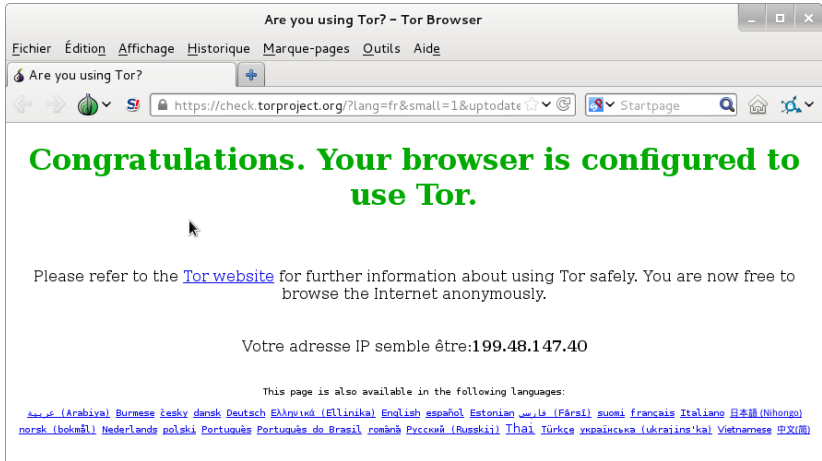
Le Tor Browser est une version Extended Support de Firefox, auxquelles sont ajoutée les extensions préconfigurées permettant qu'au lancement du navigateur, celui-ci se connecte à Tor.

⇒ Ainsi, toute la navigation qui se fait via ce navigateur est faite au travers du réseau Tor.

⇒ C'est simplissime.

Toutes les versions (dans différentes langues, différents OS) sont disponibles sur le site du projet : <https://www.torproject.org/projects/torbrowser>

Le Tor Browser



Tor Browser Launcher

Pour avoir un Tor Browser toujours à jour, on peut installer le Tor Browser Launcher. <https://github.com/micahflee/torbrowser-launcher>

Il gère :

- le téléchargement de la version la plus récente de TBB, dans votre langue et pour votre architecture
- la mise à jour automatique (tout en conservant vos signets et préférences) manuel
- la vérification de la signature GnuPG du TBB (pour être sûr de l'intégrité des fichiers)
- ajoute un lanceur d'application "Tor Browser" dans le menu de votre environnement de bureau.

Utiliser Tor - Tails

Tails est un système d'exploitation complet basé sur Linux et Debian, en live.

The screenshot shows the Tails website interface. At the top, there's a navigation bar with 'news' and 'Appel à tester Tails 0.19-rc1'. The main heading is 'Appel à tester Tails 0.19-rc1'. Below it, a paragraph explains the purpose of the test version. A list of links is provided: 'Comment tester Tails 0.19-rc1 ?', 'Quoi de neuf depuis la 0.18 ?', and 'Problèmes connus dans la version 0.19-rc1'. A green button 'Télécharger Tails Tails 0.18' is visible on the right. Below the heading, a section titled 'Comment tester Tails 0.19-rc1 ?' contains a list of instructions. The first instruction is to download the ISO and signature, with corresponding green buttons. The second instruction is to verify the ISO. The third instruction is to check for problems, with links to 'problèmes connus de cette version' and 'problèmes connus de longue date'. The fourth instruction is to test the system. The fifth instruction is to report problems, with links to 'rapporter', 'points bonus si vous vérifiez que ce n'est pas un problème connu de cette version', and 'problème connu de longue date'. A sidebar on the right contains links: 'À propos', 'Premiers pas...', 'Documentation', 'Aide & Support', and 'Participer'. At the bottom, there's a section 'Quoi de neuf depuis la 0.18 ?' with a link to 'Nouvelles fonctionnalités' and a version number 'Linux 3.9.5-1'.

Tails
The Amnesic Incognito Live System

news Appel à tester Tails 0.19-rc1

Français (63 %) EN DE ES PT

Appel à tester Tails 0.19-rc1

Vous pouvez aider Tails ! La première (et on espère seule) version candidate pour la version 0.19 à venir est sortie. Merci de la tester et de voir si tout fonctionne pour vous.

- 1. [Comment tester Tails 0.19-rc1 ?](#)
- 2. [Quoi de neuf depuis la 0.18 ?](#)
- 3. [Problèmes connus dans la version 0.19-rc1](#)

Comment tester Tails 0.19-rc1 ?

1. Gardez à l'esprit que c'est une image de test. Nous nous sommes assurés qu'elle n'est pas corrompue d'une manière évidente, mais elle peut toujours contenir des problèmes non découverts.
2. Téléchargez l'image ISO et sa signature :
 - [Image ISO de Tails 0.19-rc1](#)
 - [Signature de Tails 0.19-rc1](#)
3. Vérifiez l'image ISO.
4. Jetez un oeil à la liste des [problèmes connus de cette version](#) et à la liste des [problèmes connus de longue date](#).
5. Testez à volonté !

Si vous découvrez quelque chose qui ne fonctionne pas comme prévu, merci de [nous le rapporter](#) ! Points bonus si vous vérifiez que ce n'est pas un [problème connu de cette version](#) ou un [problème connu de longue date](#).

Quoi de neuf depuis la 0.18 ?

- Nouvelles fonctionnalités
 - » Linux 3.9.5-1.

[Télécharger Tails Tails 0.18](#)
Dernière version : 18 mai 2013

À propos
Premiers pas...
Documentation
Aide & Support
Participer

Tor hidden service - les services cachés de TOR

Tor permet aux clients et aux relais d'offrir des services cachés. Il est possible d'offrir un serveur web, un serveur SSH, etc, sans révéler son adresse IP aux utilisateurs.

- Tous ces sites ne sont accessibles que via le réseau Tor.
- Ils portent une adresse qui se termine par .onion.
- Des wikis et moteurs de recherches référencient ces services.

Soutenir Tor

Il existe l'association NosOignons.net, qui propose des nœuds de sortie Tor financés par la communauté. <https://nos-oignons.net>

- En parler
- Faire un don
- Mettre en place un relais

Sur Internet, si c'est gratuit,
c'est vous le produit

Qu'est-ce que le pistage ?

Le pistage sur Internet

- Le pistage est un terme qui comprend des méthodes aussi nombreuses et variées que les sites web, les annonceurs et d'autres utilisent pour connaître vos habitudes de navigation sur le Web.
- Cela comprend des informations sur les sites que vous visitez, les choses que vous aimez, n'aimez pas et achetez.
- Ils utilisent souvent ces données pour afficher des pubs, des produits ou services spécialement ciblés pour vous.

Comment est-on tracké ?

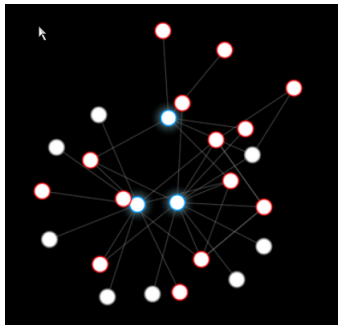
Toutes les publicités nous espionnent

- Le bouton Like de Facebook : il permet à FaceBook de savoir que vous avez visité ce site, même si vous n'avez pas cliqué sur ce bouton.
- Même si vous vous êtes correctement déconnecté de Facebook.
- De même pour le bouton le +1 de Google, les scripts de Google Analytics,
- Tous les publicité, Amazon...



L'extension Firefox LightBeam (ex Collusion)

Cette extension permet de voir en temps réel qui nous traque et les interconnexions qu'a le site actuellement visité avec d'autres sites.



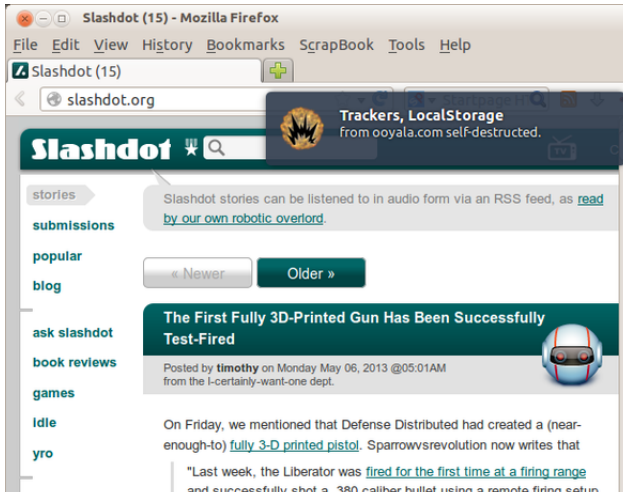
Anonymat et extensions pour Firefox

Noscript

Bloque tous les trackers associés au site.

Self destructing cookie

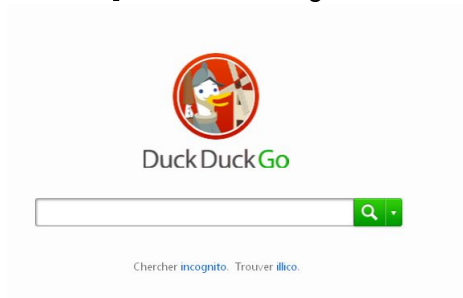
Suppression automatisée des cookies



Changer de moteur de recherche

Duckduckgo - Google tracks you. We don't.

`https://duckduckgo.com/`



Et pour plus de sécurité ?

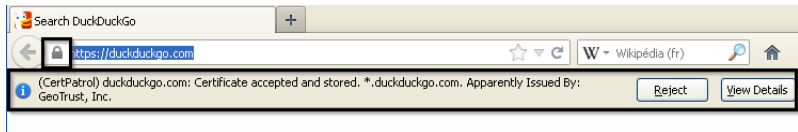
HTTPSEverywhere

Force le passage en https quand celui-ci est proposé par le site.



Certificate Patrol

Permet de valider les certificats d'un site (lié à https).



Something unclear?



Feel free to ask for questions now.

Crypto-anarchy

Everyone does encryption and what is really important is encrypted and embedded in it.

It creates noise which prevents mass surveillance (PRISM ...)

Attention ! At the current time, encryption is not widespread, anyone who encrypt its e-mails can be considered as suspicious.

Relativity of anonymity today

Analysis on language elements

- We can identify someone by studying the typography, style, vocabulary, culture, ideas ..
- the frequency of words used, the turn of phrase, the kind ...
- Theses techniques are used to determine who hides behind...
Anonymous

Care of Logs

- Schedules connections times and estimated time zone also provide information ...

Something unclear?



Feel free to ask for questions now.

Rendez vous at the Cryptoparty

CRYPTOPARTY