Les Chiffrofêtes

Genma

20 février 2014

This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.

Les Chiffrofêtes

Qu'est ce qu'une chiffrofête ?

Chiffrofête, cryptopartie...

- Le terme de cryptoparty (contraction de crypto - chiffrement et party - partie, fête) est souvent francisé en cryptopartie mais nous utilisons le terme de chiffrofête (contraction de chiffrement et fête) qui se veut une traduction moins connoté de ce terme.
- L'autre appellation que nous utilisons pour ce même type d'évènement étant les Café vie privée.

Rien à cacher

Que répondre à Je n'ai rien à cacher ?

- xx

Le public concerné

Quel est le public ciblé/concerné par les chiffrofêtes ?

Le public est divers et varié :

- Journalistes
- Scolaires (Lycéens, étudiants)
- Grand public (tout âge confondu)

D'une façon générale, ce peut être toute personne sensibilisée / concernées par les problématiques de la vie privée, de la sécurisation de ses communications...

Ateliers

Quels sont les ateliers possibles ?

- OTR “off the record”
- TOR : Présentation de Tor, Utilisation via le Tor Browser bundle et/ou le live-cd Tails
- TrueCrypt : Présentation, Création d’un conteneur chiffré, Utilisation avancée (Conteneur caché)
- GPG : Thunderbird et Enigmail, création et gestion des clefs, réseau de confiance...
- Le tracking sur Internet : utilisation d’extensions pour Firefox
- Darknet : I2P etc.
- Crytpoavancée : chiffrement de serveurs, TAHOELFS...

Les logiciels

Quels logiciels ?

Les outils présentés sont donc tous compatibles Linux, Windows et Mac et/ou y possèdent des alternatives, et on parle aussi des problèmes rencontrés sur mobile.

Mini-conférences et conférences

Mini-conférences et conférences

- Au cours d'une chiffrofête, une ou plusieurs conférences peuvent être présentées au public.
- La présentation d'une conférence peut être indépendante de l'organisation d'une chiffrofête et les conférences peuvent être regroupées/fusionnées pour faire une conférence globale abordant différents thèmes au cours d'une après-midi ou sur une journée entière par exemple.

Organiser

Qui peut faire une chiffrofête ?

- Toute personne qui a les connaissances minimales et qui souhaite les partager peut se lancer dans la mise en place de sa propre chiffrofête.

Logistique

Quelle est la logistique d'une chiffrofête ?

Les éléments suivants ont été identifiés :

- connaitre la capacité d'accueil du lieu, avoir un ou plusieurs contacts référents
- prévoir une inscription en ligne (pour évaluer le nombre de participants) sur un outil permettant l'anonymat
- prévoir un accès à Internet via un réseau filaire (câbles ethernet + switch) et/ou Wifi.
- prévoir chaises, tables, rallonges électriques en quantité suffisante
- un vidéo-projecteur

Le lieu

Quels sont les lieux susceptibles d'accueillir une chiffrofête ?

- Les chiffrofêtes étant destinées à un public varié, du grand public aux utilisateurs plus avancé, les lieux peuvent être des médiathèques, des salons informatiques...

Communication

Quelques slogans peut-on utiliser pour promouvoir les chiffrofête ?

- Venez apprendre à protéger vos communications en ligne !
- Chiffrement et anonymat : reprenez le contrôle de votre vie privée.
- Surfez et chattez couverts avec des cypherpunks gentils.

Ou encore

- Parce que préserver sa vie privée est un droit,
- Parce qu'on peut avoir envie de ne pas être espionné,
- Parce que l'on a TOUS quelque chose à cacher,
- Parce que les outils existent et ne sont pas si compliqués...
- Venez apprendre à vous protéger en ligne !

Des conseils

Quelques conseils pour le déroulement de la chiffrofête ?

- S'adapter au niveau des participants (du débutant à l'utilisateur avancé)
- Prendre en compte des besoins et des attentes du public.
- En début de séance, un petit sondage/tour de table permet de définir les attentes et les ateliers qui seront
- La durée conseillée pour les ateliers est de 1h30.
- Deux ateliers successifs semblent suffisant pour commencer (cela fait 3h avec une pause entre les deux).

Les Chiffrofêtes et le logiciel libre ?

Le logiciel libre

Et le logiciel libre dans tout ça ?

- Dès que possible, c'est le logiciel libre qui est privilégié. Chacun vient avec son ordinateur et quelque soit le système d'exploitation (GNULinux, MacOSX, Windows, Android), les logiciels les plus adaptés sont proposés, installés.
- Mais Apple, Windows et Android posent le soucis de ne pas être des systèmes libres, donc on ne peut pas leurs faire confiance.
- Faire de la crypto là-dessus, c'est un peu comme avoir une porte blindée à sa maison, mais des murs en carton-pâte.

Le logiciel libre

Le libre, le libre, le libre...

- On incite donc fortement à utiliser uniquement des choses libres, GNU/Linux ou alternatives à Android (Replicant, CyanogenMod).
- Windows et Apple sont plus que fortement déconseillés dans le contexte de la confiance et de la crypto.

Conclusion

Les réserves

La crypto forte sur téléphone

- On ne sait juste pas ce qui se passe directement au niveau des puces qui gère la radio (les « fameux » baseband).

Les limites

- Le chiffrement ne fait pas tout (il faut faire les mises à jours...)
- Il y a aussi l'OPSec...

Merci de votre attention.
Place aux questions. Débattons...