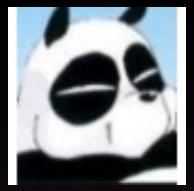
Des cryptoparty au Café vie privée, le chiffrement est en pleine démocratisation

Genma



A propos de moi

Où me trouver sur Internet ?

- Le Blog de Genma :
  http ://genma.free.fr
- Twitter :
  http ://twitter.com/genma

Mes centres d'intérêts ?

Plein de choses dont :

- La veille technologique
- Le chiffrement

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.
  - Connoté au sens où cryptoparty est très lié au monde des hackerspaces, underground...
- L'autre appellation que nous utilisons pour ce même type d'évènement est les Cafés vie privée.

Quand cela a-t-il commencé ?

- Les cryptoparty existent depuis longtemps. Mais c'est en octobre 2013, à l'intiative, entre autre d'Amaelle Guiton et d'Okhin qu'a été lancé le premier Café vie privée.
- Et c'est en novembre 2013, lors de l'Ubuntu Party et des ateliers Prism Break qu'Okhin a appelé ça des chiffrofêtes.

Depuis, au moins un évènement au lieu tous les mois.

Le public concerné

Quel est le public ciblé/concerné par les chiffrofêtes ?

Le public est cible des chiffrofêtes est divers et varié :

- Les journalistes et autres professions à risques ;
- Ls scolaires (Lycéens, étudiants) ;
- Les geeks, libristes et autres technophiles ;
- Mais surtout Grand public (tout âge confondu).

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

Comment ça se passe ?

Le concept des chiffrofêtes

Il suffit d'un lieu où se réunir, d'animateurs désirant partager leurs connaissances et d'un public désireux d'en savoir plus, qui a envie d'apprendre.

Ateliers, conférences, débats

Au début, on fait une rapide présentation des sujets qui peuvent être abordés. Ensuite, des groupes se forment et se déroulent alors :

- une mini-conférence/un talk de présentation ;
- un atelier (chacun installe et manipule sur ma machine) ;
- un débat/scéance de questions réponses.

La durée idéale est d'une heure et demi. Avec deux scéances, on remplit un après-midi.

Les logiciels 1/2

Le logiciel libre

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.

- 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.

Les logiciels 2/2

Le logiciel libre suite

- Windows et Apple sont plus que fortement déconseillés dans le contexte de la confiance et de la crypto.
- Faire de la crypto là-dessus, c'est un peu comme avoir une porte blindée à sa maison, mais avec des murs en carton-pâte.

Nous réfléchissons à mettre en place des sessions de type Install party pour mettre des doubles boot...

Les ateliers proposés

- Comment chiffrer ses emails avec GPG ;
- Savoir surfer anonymement et utiliser TOR (Tails, TorBrowser Bundle) ;
- Protéger son navigateur et comprendre les certificats de sécurité (SSL) ;
- Comprendre et utiliser un VPN ;
- Protéger ses communications et son surf. Laptop et smartphone en nomade (wifi et outils) ;
- Protéger ses informations avec TrueCrypt ;
- Mots de passe et identification multi-facteurs ;
- Identifier et savoir gérer ou effacer les métadonnée...

Tout ce qui a un lien avec la vie privée...

Organiser des chiffrofêtes

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.

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...

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 suffisant ;
- un vidéo-projecteur...

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 mis en place.
- 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).
- Attention aux photos/enregistrements etc.

Et si vous vous lanciez à votre tour ?

Comment aider, contribuer...

Lancer vous dans votre ville, votre association, LUG.... Parlez-en autour de vous.

Les problématiques autour des chiffrofêtes

Quelques problématiques...

Peut-on conseiller de chiffrer sur des OS privateurs ?

Il faut présenter tous les outils avec toutes leurs limites. Et considérer que la personne en face est assez intelligente pour choisir.

L'ergonomie des logiciels

Les projets comme Tor, Tails... font des sessions sur l'amélioration du design de l'expérience utilisateur. Le soft doit s'adapter à l'utilisateur et non l'inverse.

Quelques problématiques...

Création d'un faux sentiment de sécurité

Quelques clics peuvent permettre d'envoyer des mails chiffrés (Enigmail). Mais on oublie la problématique des métadonnées associées, qui sont les données réellement importantes...

Le threat model

Chacun a un threat model/modèle de menace différente et le curseur du niveau de sécurité nécessaire ne sera pas le même...

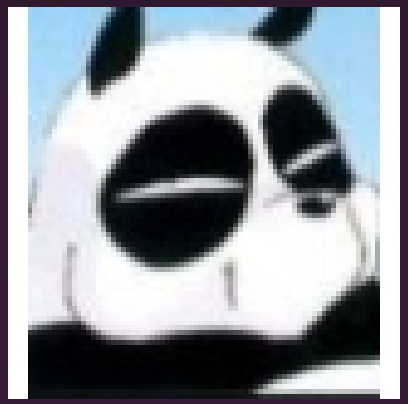
Et d'autres problématiques qui peuvent-être abordées dans les questions

Conclusion

Participez à la chiffrofête

Tous les jours, au RDC

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



- Le Blog de Genma
  http ://genma.free.fr
- Twitter @genma