GPG signature et chiffrement

GnuPG

Logiciel Libre pour la signature et le chiffrement des mails et/ou des fichiers

Root66.Net
http://www.root66.net/

Sima78
http://chispa.fr/sima/

GPG signature et chiffrement

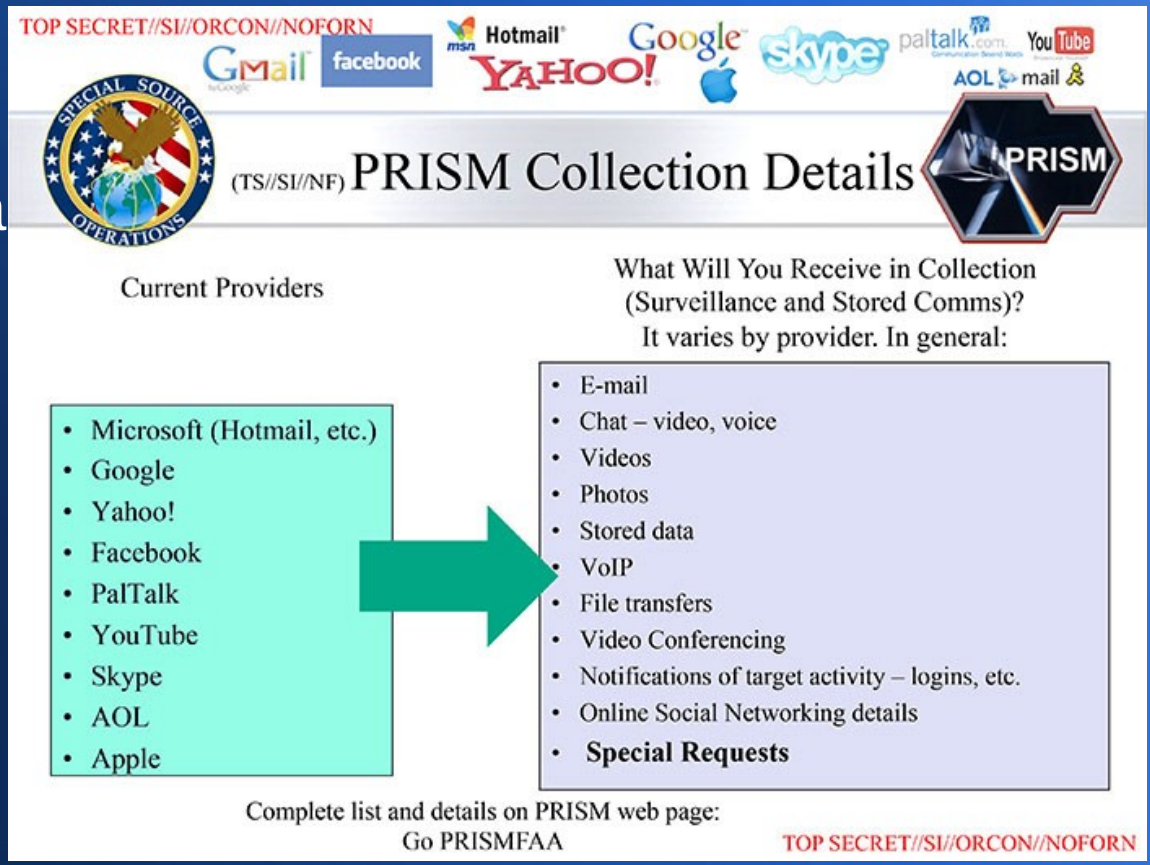
EN TROIS TEMPS

- 1er temps – Les grandes généralités.
- 2ème temps – Pause café/gâteaux.
- 3ème temps – Questions/réponses

Faut-il chiffrer ses mails ?
L'espionnage au quotidien : PRISM

Les journaux anglosaxons The Guardian et le Washington Post du 7 juin 2013 ont révélé une affaire d'espionnage des citoyens à l'échelle internationale : **le programme PRISM.**

Vous avez un compte sur Yahoo, Hotmail (Live Mail) ou Gmail, vous communiquez par e-mail et avez une liste de contacts, vous communiquez par GSM, êtes actifs sur Facebook, communiquez votre position GPS ou tchater sur Skype ? Sachez que dorénavant l'Oncle Sam vous écoute et vous lit !



Faut-il chiffrer ses mails ?

Edward Snowden, Citizenfour, 2014

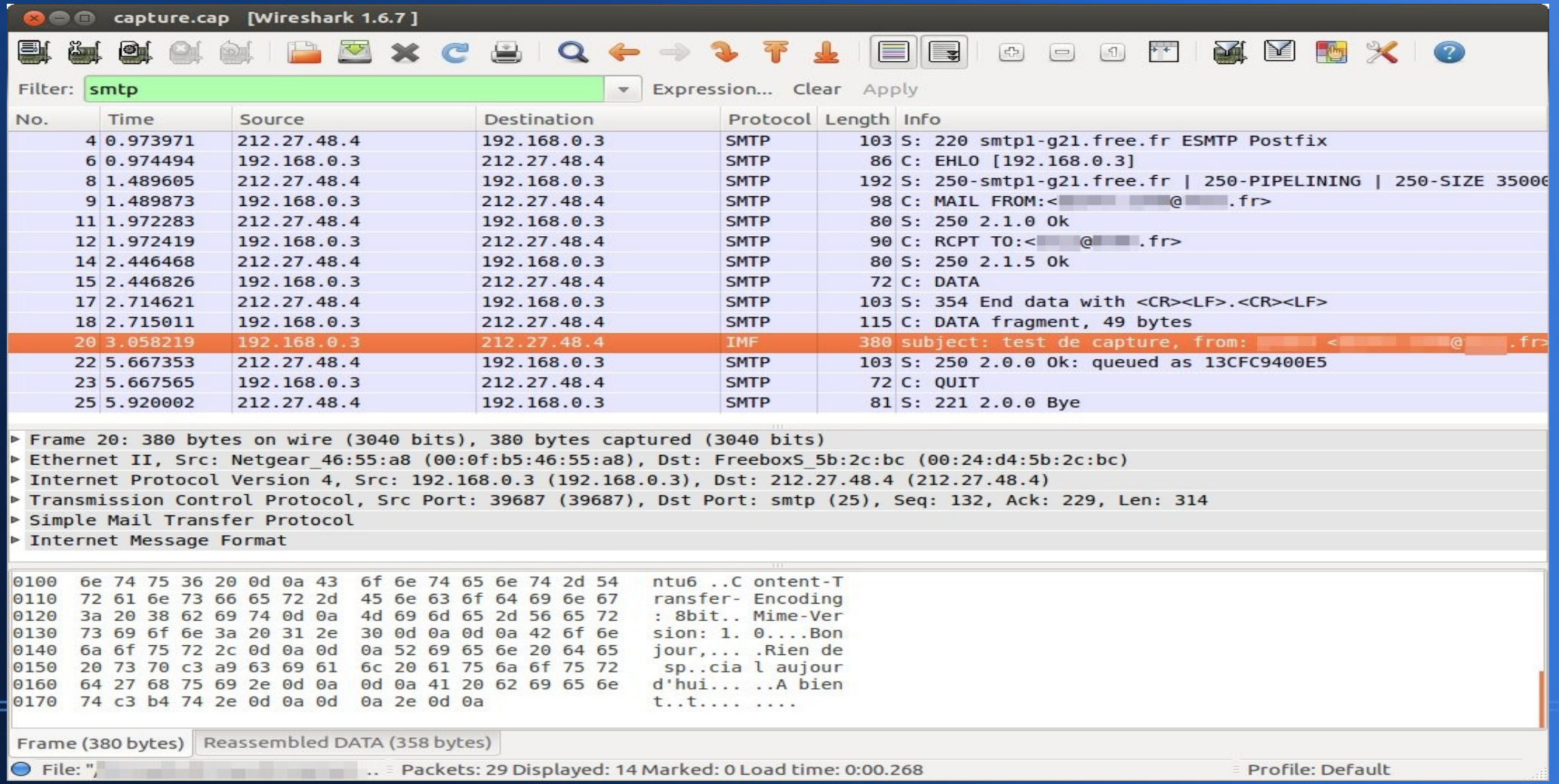
Lorsque vous dites
'le droit à la vie privée ne me préoccupe pas, parce que je n'ai rien à cacher',
cela ne fait aucune différence avec le fait de dire
'Je me moque du droit à la liberté d'expression parce que je n'ai rien à dire'.

Faut-il chiffrer ses mails ?

- **SMTP**, Simple Mail Transport Protocol
- Transit des données est en clair
- Les intermédiaires sur le réseau voient vos données et peuvent les lire !
- Une confidentialité similaire à une carte postale

Démonstration avec wireshark

- # tcpdump -i eth1 port 25 -vvv -w /root/capture.cap



Notions basique de cryptographie

- Cryptographie symétrique

•Cryptographie symétrique

Solutions simples

- On choisi une méthode (ex : décalage de 15 lettres les lettres de chaque mot
- On choisi un algo et un mot de passe (XOR, DES, ROT13, AES …)
  - ↗ Méthode puissante de chiffrage
  - ↘ Comment donner le mot de passe si on ne se voit pas ?
  - ↘ Un seul mot de passe, comment être certain qu'aucun de nos contacts ne diffusera le mot de passe ?

Notions basique de cryptographie

- Cryptographie symétrique
- Cryptographie asymétrique

Cryptographie asymétrique

Fonctions mathématiques à sens unique, ou très difficile à inverser, basée sur le principe d'échange de clé (Diffie Helmann, 1976) dont une première implantation en 1978 sous le brevet RSA (Rivest, Shamir et Adelman)

- Chaque partie possède **deux** clés
  - une clé **privée**, que l'on garde secrète
  - une clé **publique**, diffusée à tout le monde

Notions basique de cryptographie

- Cryptographie symétrique
- Cryptographie asymétrique
  - Gnupg est basé sur la cryptographie asymétrique.
  - Point faible : le mot de passe. Il faut un mot de passe « fort ! »

La paire de clés

Pour signer ses mails et les chiffrer, il faut

- Être au moins deux 

Générer une paire de clés

- Une sera publique, donc accessible à tous !
- L’autre sera privée, donc jamais diffusée !

On génère aussi une clé de révocation, nous verrons plus loin dans la présentation...

L'importance de la signature

Signer les messages envoyés… La signature !

- Elle permet de pallier à l'absence d'authentification de SMTP
- N'importe qui peut envoyer des messages avec n'importe quelle adresse
- Pour avoir une garantie sur l'expéditeur du courrier

Message signé (exemple)

- Lorsque vous avez la clé publique de l'expéditeur et que vous l'avez signé, vous avez un message comme ci-dessous ou similaire :

- Signature valide (nom <adresse-mail@fai.fr>)
- Dans le cas contraire annonce d'adresse non valide et bandeau rouge au lieu du vert.

GnuPG pratique

- Pierre a 2 clés, une publique et une privée
- Sophie a 2 clés, une publique et une privée
- Pierre et Sophie se connaissent très bien.

Échanges de clés

- Pierre envoie sa clé publique sur un serveur de clés.
- Sophie envoie sa clé publique sur un serveur de clés.
- Chacun récupère la clé publique de l’autre.
- Sophie grâce à sa clé privée, signe la clés publique de Pierre après l'avoir récupéré
- Pierre grâce à sa clé privée, signe la clés publique de Sophie après l'avoir récupéré.

Échanges de clés

Pierre envoie sa clé publique

Serveur de clés

Sophie va chercher la clé publique de Pierre.
Sophie utilise sa clé privée pour signer la clé publique de Pierre.

Sophie envoie sa clé publique

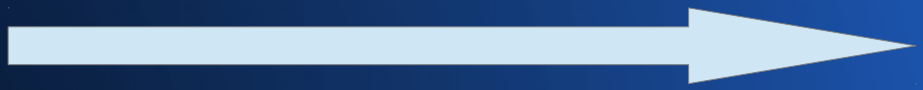
Pierre va chercher la clé publique de Sophie.
Pierre utilise sa clé privée pour signer la clé publique de Sophie.

Possibilité de s'échanger directement les clés

Envoi de message signé

- Pierre envoie un message à Sophie qu'il signe avec sa clé privée
- Sophie vérifie avec la clé publique de Pierre et est contente, elle est certaine que c'est bien Pierre qui lui a envoyé le message

Pierre envoie un message signé



Sophie vérifie la signature

Envoi de message chiffré

- Sophie envoie un message chiffré avec la clé publique de Pierre

- Pierre déchiffre le message avec sa clé privée

Sophie envoie un message chiffré

Pierre utilise sa clé privée pour déchiffrer le message

Envoi de fichier chiffré

- Pierre envoie une pièce jointe chiffré avec la clé publique de Sophie

- Sophie déchiffre la pièce jointe avec sa clé privée

Pierre envoie un fichier chiffré

Sophie déchiffre le fichier reçu

ATTENTION, lors d'envoi d'un message chiffré, les pièces-jointes ne sont pas chiffrées... Il faut chiffrer les fichiers avant de les joindre ! En fonction de la messagerie utilisée.

Chiffré un fichier pour soi

- Sophie souhaite garder ce fichier lisible que pour elle-même.
- Elle le chiffre avec sa clé privée (après l'avoir rendu lisible).
- Et le sauvegarde sur son disque dur.

Sophie après avoir vu le fichier, le chiffre pour elle-même et le sauvegarde.

À savoir : Pour garder des fichiers lisibles que pour soi, il existe d'autres méthodes plus appropriées

Signer une clé, oui mais...

- La signature sert a identifier un expéditeur
- N'importe qui peut créer une clé publique avec le nom de n'importe qui
- Solution: **Le réseau de confiance**
  - Nous verrons plus loin...

D'où vient la clé publique ?

- de vive voix
- grâce à sa carte de visite papier,
- par téléphone (une personne malveillante n'aura pas la même voix),
- Lors d'une "signing party"
- ✗ Typiquement pas par mail, puisqu'une personne malveillante peut se faire passer pour quelqu'un d'autre.

Echanges de clés

Pour réaliser un échange de clé sécurisé il faut donc:

- S'échanger les cartes de visites en vérifiant les identités.
- Récupérer la clé dont l'identifiant se trouve sur la carte de visite.
- vérifier que le fingerprint calculé à partir de cette clé est identique à celui imprimé sur la carte de visite.
- Signer la clef.

Exemple de carte d'échange

M. Trucmuche Georges

- Clé : 0C39ACCC
- Empreinte de la clef :

  4700 6F08 3B93 A0DA E0AE 463D 2F00 198A 0CAC 39CC
- uid Trucmuche <trucmuche@fai.fr>

Niveau de confiance

- Lorsque l'on signe une clé nous pouvons lui donner un niveau de confiance :

  1 = je ne sais pas ou n'ai pas d'avis

  2 = je ne fais PAS confiance

  3 = je fais très légèrement confiance

  4 = je fais entièrement confiance

  5 = j'attribue une confiance ultime

Réseau de confiance

- Les utilisateurs **signent les clés** d'autres utilisateurs dans lesquels ils ont confiance
- Permet de voir qui a signé la clé, qui a confiance en cette clé.
- Repose sur le facteur humain,donc faillible

Questions ? / Réponses ?

Questions ? / réponses ?

Et / ou

Pause café ?

Pour aller plus loin

Applications graphiques :

- KGpg
- GnomePGP
- Seahorse
- Kleopatra
- ...

Les softwares

- Linux, BSD, ... : Gnupg
- Windows : GPG4win
- MAC : GPGMail ou GPGSuite

Messageries pouvant utiliser GnuPG

- Courriel sous linux :
  - Evolution / Kmail / Claws Mail (ancien Sylpheed)
- Courriel sous Linux/Windows/MAC (L/W/M)
  - Thunderbird
- Messagerie instantanée (L/W/M) : Jabber - Gajim
- Courriel sous Windows
  - Pegasus Mail / Becky! 2 / MS-Outlook / MS-Outlook Express 5.x / 6 / Eudora

Serveurs de clés

- http://keyserver.ubuntu.com/
- http://keys.gnupg.net/
- http://pgp.mit.edu/
- http://keyserver.pgp.com/
- http://subkeys.pgp.net:11371/
- http://pool.sks-keyservers.net:11371/

Les serveurs sont généralement connectés entre-eux, donc il suffit d'envoyer votre clé à un seul serveur.

Liens utiles

- http://www.gnupg.org/howtos/fr/
- http://www.francoz.net/doc/gpg/

Créer votre carte de visite

- http://openpgp.quelltextlich.at/slip.html
- utiliser l'outil gpg-key2ps du paquet signing-party

En savoir plus sur la cryptographie

- http://fr.wikipedia.org/wiki/Cryptographie_sym%C3%A9trique
- http://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique