Quelques notions de sécurité à destination du chercheur non informaticien

Plan

- Sécurité : pourquoi ?
- réseau, wifi
- Certificats, https
- téléphones mobiles
- Protection physique (mot de passe bios, chiffrement du disque dur)
- gestion des mots de passe
- sécurité des portables et du navigateur WeB (principalement orienté sur firefox et chrome : flash, javascript, pdf, …)
- bonnes pratiques (mail, formats de documents) où comment transmettre sans le vouloir des informations confidentielles

Sécurité : pourquoi ?

- Confidentialité de votre travail, de votre messagerie, des coordonnées de vos contacts
- Usurpation : faire des choses illégales en votre nom
- Rebond/botnets : utiliser votre installation informatique sans votre accord
- Ransonware : chantage à la perte de données

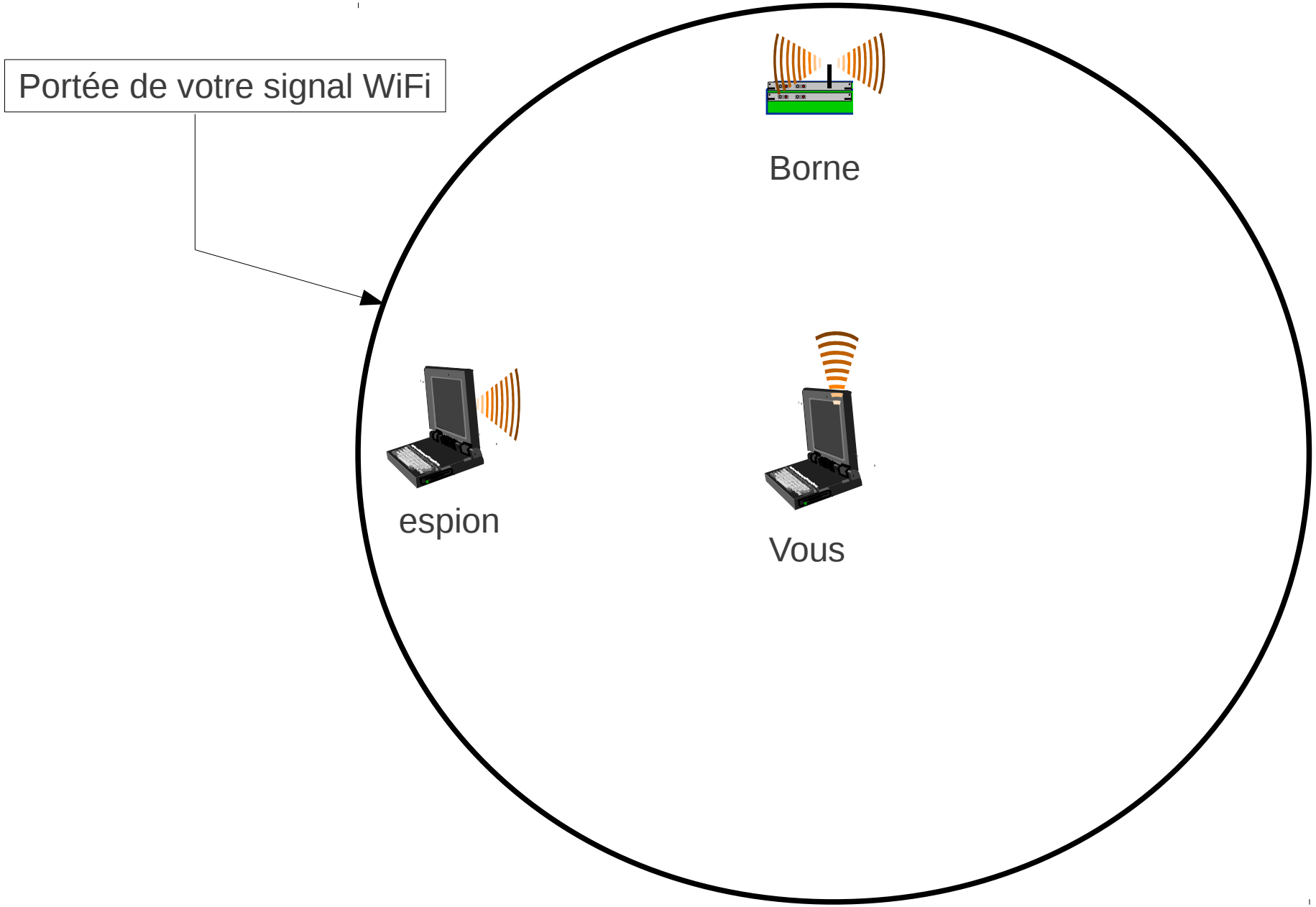
On vit dans un monde formidable !

- Regardons un bulletin du CERT RENATER
- http://sites.univ-provence.fr/wcri/d_serv/d_reseau/d_cert/courant/certmsgSTAT13

WiFi : enjeux

- Utilisation du réseau par un utilisateur non légitime
  - Pour rebond
  - Pour réseau local
  - Pour attaque des autres postes WiFi
    - Solution : interdire les connexions entre postes WiFi (réglage point d'accès)
- Espionnage des données échangées :
  - Sites consultés
  - Mot de passe
  - ...

WiFi : enjeu



WiFi : sécurité

- Ouvert : pas de chiffrement. En général associé à un portail d'authentification
- WEP : chiffrement MAIS cassable en quelques minutes par tout clampin
- WPA1/WPA2 personnal : chiffrement solide (si clef solide) MAIS clef commune
- WPA2 entreprise + 802.1X + méthode génératrice de clef : chiffrement solide, clef unique par poste
- Exemples : google cars.
- Solutions
  - https plutôt que http
  - VPN

Solutions : http/https

- Utiliser https partout où c'est possible
  - Trafic chiffré entre votre navigateur et le serveur
  - Authentification du serveur
- Extension firefox : httpseverywhere (https://www.eff.org/https-everywhere)

Certificats, https

Carte d'identité

Pascal PETIT

Certificats, https

Certificats :

- Un certificat :
  - Identité,
  - clefs publique
  - Certifiés par une autorité de certification
- Permet l'authentification d'un site
  - Le site possède la clef privée associée
  - Le site indiqué par le certificat est bien celui auquel on se connecte
- Permet la mise en place d'un tunnel chiffré : protège contre l'espionnage des communications

certificats et hameçonnage

- Du phishing pour identifier les opposants à Bachar El-Assad
  - faute site youtube annonçant une fausse mise à jour de flash
    - => installation d'un logiciel espion
  - faux site facebook ou youtube
    - récupérer login et mot de passe (y compris des personnes qui mettent des commentaires)
- source : Numerama, 30 mars 2012 :
  http://www.numerama.com/magazine/22197-du-phishing-pour-identifier-les-opposants-a-bachar-el-assad.html

limite de https

- vigilance des utilisateurs (cf exemple syrien)
- fiabilité des autorités de certification
  - que penser d'une AC liée à un pays
  - impact possible
    - créer un faux certificats reconnu comme valide par le navigateur
    - l’hameçonnage sans détection possible
- solutions :
  - aucune
  - une idée : associer les certificats de sociétés connue à des AC et refuser les certificats signés par d'autres AC
  - revient à refuser une carte d'identité d'un français si elle est validée par la Grande Bretagne

smartphones

- des téléphones aux usages variés qui induisent de nouveaux risques
  - photos
  - données (le tel. sert souvent de clef USB)
  - données personnelles
  - accès aux comptes mails & Co via les applications ou les caches locaux
- Les risques
  - vol du téléphone
    - accès aux données présentes dans le tel. (photos, données, ...)
    - accès aux comptes mails & Co depuis le tel.
    - utilisation du téléphone
  - ver, virus & Co
  - application frauduleuse

Vol du téléphone :

- il faut rendre le tel. et ses accessoires (carte mémoire) inexploitables en cas de vol ou d'emprunt
  - code au déverrouillage
  - effacement des données en cas de code incorrect
  - chiffrement des données
  - limiter les données stockées sur le tel.
- récupérer son tel. :
  - installer des applications dédiées (géolocalisation, prise de contrôle à distance, …)
  - exemple : cerberus sous android

Vers/virus & Co

- modèle de sécurité des mobiles
  - limite grandement les problèmes

Applications frauduleuses

- frauduleuses ou pas. Comme le dit l'adage :
  - si le service est gratuit, c'est que vous n'êtes pas le client mais la marchandise
  - cet adage est particulièrement vrai de nos jours :
    - google, facebook
    - les applications gratuites sur mobile ou autre
- applications frauduleuses qui piratent vos données personnelles
- exemples : cf http://www.ecrans.fr/iPhones-beaucoup-trop-d-applis,14100.html
  - l'application ratp
  - twitter,path : tout le carnet d'adresse est collecté

mars 2011 : l'application RAPT

- cf http://www.rfc1149.net/blog/2012/03/20/a-qui-la-ratp-vend-elle-nos-informations-personnelles/
- en résumé : sans avoir prévenu, l'application envoie les informations suivantes à un publiciste :
  - user_position: notre position
  - uphone: +3365970xxxx; le No de tel. complet du tel.
  - imei: 35479504154xxxx; l'imei
  - carrier: votre opérateur
  - ugender, uage, uemail, uzip, unick: non renseignés; heureusement, l'application n'a pas réussi à récupérer les informations de sexe, âge, adresse de messagerie, code postal et pseudonyme.

mars 2011 : l'application RAPT

- comme le signale Samuel Tardieu, l'application RAPT demande des permissions pas forcément déraisonnables :
  - la possibilité de vous localiser : c'est compréhensible pour pouvoir vous guider jusqu'à l'arrêt de transports en commun le plus proche ;
  - l'accès à Internet : indispensable pour récupérer les horaires et les informations à jour ;
  - les informations de contact et l'identité du téléphone : certaines applications les utilisent pour construire un identifiant anonyme, ne permettant pas de vous identifier, mais autorisant le serveur à recouper vos requêtes à des fins statistiques.

téléphone mobile : iphone

- Mac Affee a publié 10 conseils de sécurité pour possesseurs de matériel Apple :
  - cf http://www.mcafee.com/us/resources/white-papers/foundstone/wp-top-10-iphone-security-tips.pdf

téléphone mobile android

- mot de passe au verrouillage
- chiffrer le contenu du tel.
- n'installer que des applications
  - du market/playstore
  - ayant été téléchargées par un nombre important de personnes
  - en vérifiant la cohérence des demandes d'autorisation par rapport aux fonctionnalités
- installer un logiciel de prise de contrôle à distance comme cerberus

Dropbox

- avril 2011 : changement des conditions d'utilisation de dropbox
- avant, dropbox vantait la qualité de son chiffrement AES 256bits
- détection de doublon
  - pour gagner de la place
  - suppose que dropbox puisse déchiffrer les fichiers chiffrés
- BIBLIO :
  - http://www.cnetfrance.fr/news/dropbox-induisait-en-erreur-sur-la-confidentialite-des-donnees-et-le-cryptage-39760824.htm

Dropbox : solution

- chiffrer les données soit même
- via true crypt :
  - pénible car suppose le transfert de tout le contener à chaque modification
  - soit avec des solutions fichiers par fichiers à la encfs
    - pcimpact : http://www.pcinpact.com/dossier/chiffrement-cloud-encfs-boxcryptor-dropbox/209-1.htm
    - http://korben.info/dropbox-chiffrer-crypter-securiser.html
    - http://korben.info/boxcryptor-dropbox-crypte.html
    -

Protection des disques durs

- Mot de passe du bios
  - Peut être supprimé par un voleur
  - Ne l'utiliser que pour empêcher l'utilisation du portable en votre absence
- Mot de passe du disque dur
  - Le mot de passe est stocké dans l'électronique du disque
  - Beaucoup plus résistant
  - Plusieurs niveaux de sécurité (récupérable par le constructeur ou non)
- Chiffrement de partitions ou de disques

Truecrypt : références

- Le FBI se serait cassé les dents dessus : http://sid.rstack.org/blog/index.php/400-pbkdf2-a-l-epreuve-du-fbi
- Rapport de certification de la version 6.0a : http://esec.fr.sogeti.com/FR/documents/presse/tc_dcssi.pdf
- Site officiel : http://www.truecrypt.org/

True crypt fonctionnalités

- Peut chiffrer un disque virtuel dans un fichier
- Peut chiffrer une partition (y compris la partition où est installé windows)
- Le chiffrement est transparent et automatique
- Permet de la stéganographie (méfiance : des travaux récents permettent de détecter les conteneurs truecrypt)
- Fournit des mécanismes de déni plausible en cas de fourniture forcée du mot de passe

encfs/box cryptor

- outils de chiffrement de dossier
- chiffre fichiers par fichiers
- plus efficace en cas de synchronisation entre dossiers sauvegardés
- les outils :
  - encfs/cryptkeeper : sous linux
  - boxcryptor : sous windows

Chiffrement : ne pas jouer avec les autorités :

- Si vous êtes épicier à Tarnac
- Si vous allez visiter un pays un peu parano
  - Ne pas cacher l'existence de données chiffrées
  - On peut vous obliger à fournir la clef de déchiffrement
  - On peut copier l'intégralité du de votre mobile, de votre portable, …
  - Dans les labos, utilité de prévoir un portable blanc remis à zéro régulièrement et ne servant qu'à ça.
- Références :
  - http://www.dgdr.cnrs.fr/fsd/securite-systemes/documentations_pdf/securite_systemes/consignes-portables-etranger.pdf
  - http://www.numerama.com/magazine/3065-la-douane-americaine-peut-fouiller-votre-disque-dur.html
  - http://www.generation-nt.com/pc-portable-douane-police-actualite-18291.html

Mots de passe

- Mots de passe différents et solides
- Hiérarchiser les mots et les contextes d'utilisation
- Pourquoi ?
  - Attaque par dictionnaire ou par force brute sur une empreinte
  - Site WeB peu scrupuleux
    - exemple de Raymond qui s'est fait piraté son compte gmail pour envoyer du spam
  - Vol de données
    - cf monster en 2009 : http://sid.rstack.org/blog/index.php/319-oops-i-did-it-again)
    - Sony récemment : http://www.ecrans.fr/PlayStation-Network-77-millions-de,12576.html
  - Des impacts différents (gestion de compte bancaire, ...)

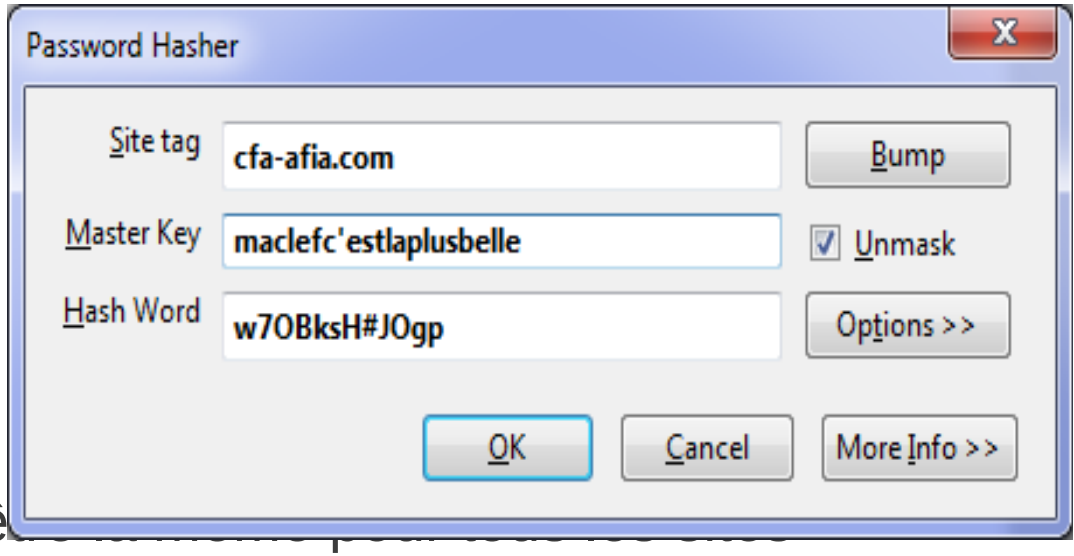
Solution :

- Changer les mots de passe par défaut des logiciels et matériels
- Sinon, vous aurez affaire à Chuck Nouris : http://www.zdnet.fr/actualites/chuck-norris-inflige-une-manchette-aux-modems-dsl-39713237.htm

Solutions : mémorisation des mots de passe par le navigateur

- Pratique
- Le fichier contenant les mots de passe doit être protégé
- Firefox :
  - mot de passe principal de sécurité
  - Sert à chiffrer le fichier contenant les mots de passe
  - il faut en mettre un
- Chrome :
  - Système similaire mais automatique
  - Attention : si on a accès à votre session, les mots de passe sont visibles dans les options de chrome
- Attention : Un attaquant qui a votre mot de passe principal a tous vos mots de passe (keyloger, ...)

Solution : hasher, hash it !



- un mot de passe
  - Différent sur chaque
  - Dépendant
    - Du site (site tag)
    - D'une clef maître qui peut ê
- Des outils compatibles :
  - Hasher pour firefox
  - passwordhasher pour chrome
  - Hash It ! Pour android
- Attention : si un intrus récupère votre mot de passe principal, il peut calculer tous vos mots de passe !

Solution : stockage sécurisé de mots de passe

- 1password
- *keyring
- Problèmes :
  - Niveau de sécurité de l'outil
  - Compromission du mot de passe principal
- Solutions :
  - Stockage sur un autre outil informatique (smartphone?)
  - MAIS gare à la sécurité sur les smartphone

Ransonware :

- Chiffrent fichiers ou disques durs
- Demandent de l'argent pour fournir la clef de déchiffrement
  - Certains sont faibles et facilement contournables
  - Les versions récentes sont très solides
- Une seule solution en cas d'infection :
  - Avoir de bonnes sauvegardes
- Exemple
  - Gpcode analysé dans un article de Nicolas Brulez de la revueMisc No 55 (mai-juin 2011)
  - Utilise de la crypto symétrique et asymétrique solides

Botnets : pourquoi, comment ?

Sécurité du poste de travail

- Impossible
- Des outils grand public qui sont durablement des passoires :
  - Produits adobe (flash, acrobat reader) : des fonctionnalités peu utiles les affaiblissent
  - Navigateurs WeB (internet explorer mais pas que lui)
  - …
- Des systèmes d'exploitation très utilisés et très attaqués
- http/https : pour éviter le sniffage réseau
- difficile de se protéger de l'équipe système qui a les moyens de mettre en place des keyloggers & Co

Solutions : http/https

- Utiliser https partout où c'est possible
- Extension firefox : httpseverywhere (https://www.eff.org/https-everywhere)

Solutions Flash :

- S'en passer:-)
  - Via le support html5 des navigateurs récents : firefox4, chrome, ie9, safari, opera)
  - Problèmes :
    - Les sites consultés doivent supporter html5
      - Youtube : supporte html5 (webM)
      - Dailymotion : supporte html5 (h264)
    - La guerre des codec video : webM (google, firefox, opera) contre H264 (ie9, safari)
  - C'est la meilleure solution mais difficile à vivre (sauf ipad & Co qui n'a pas flash:-))

Solutions Flash :

- Être prudent :
  - Pas de sites pornographiques ! Ou douteux
  - Utilisation d'outils de filtrages :
    - On active ponctuellement flash sur une video de son choix en cliquant dessus
    - Flashblock (chrome, firefox)
    - ClickToFlash (safari)
  - Mise à jour de flash
    - Chrome : intègre flash, garantit une mise à jour rapide
    - Sinon, penser aux mises à jour du Plugin

WeB : éviter les sites douteux : WebOfTrust

- un outil collaboratif
  - l'accès à un site peut être interdit s'il est considéré comme dangereux
  - on peut passer outre l'interdiction
- très facile d'accès
  - devrait être installé par défaut sur les navigateurs
- gare aux abus du collaboratif :
  - à une époque, le site de l'UMP avait été déclaré comme dangereux

WeB : noscript

- N'autorise le javascript que de certaines sources
- Rappel : une page WeB peuplée d'objets de sources variées
- Idéal contre la publicité et certaines formes de flicage
- Un peu lourd à l'utilisation
- Idéal pour la sécurité

Skype

VPN kesako ?

VPN à l'UEVE

Mail & Co : bonnes pratiques

- Mail : gare à la diffusion involontaire d'information
- Informations contenues dans les documents pdf, m$-office & Co

Mail : du danger de la citation

- Guerre de religions avec 2 sectes :
  - Le dinosaures : Ceux qui répondent au dessous du texte cité
  - Ceux qui répondent au dessus du texte cité
  - ràf : un exemple de chaque

Mail : du danger de la citation

- Citer l'intégralité du courrier auquel on répond
- Au fil des échanges, ajouter des destinataires
- => danger
- Exemple : cf ràf
- Bonne pratique :
  - Choisir sa secte (pas important)
  - Relire la partie citée
  - En supprimer les parties non pertinentes du courrier cité

mail : stockage, diffusion

- avoir accès au serveur où sont vos boîtes aux lettres permet de lire vos mails
- toute machine où passent vos mails est un point où ils peuvent être espionnés
- gmail : google analyse le contenu de vos mails pour vous profiler
- conseil : soyez paranoïaques
  - des solutions techniques et des adresses différentes selon les activités (prof. perso, syndicales, …)
  - utilisez le chiffrement des courriers

Faire parler les documents plus qu'ils ne le devraient

- Référence principale : MISC Mag HS No 3, page 40 à 49 : « Faire parler les documents plus qu'ils ne le devraient » de Frédéric Raynal et François Gaspart.
- Plan :
  - Métadonnées
    - Bureautique microsoft
    - Pdf
  - Versions
    - Pdf
    - Microsoft
  - Séparer la forme du fond : exemples à ne pas suivre
    - Cadres noirs en pdf
    - Écriture blanc sur blanc
    - Analyse de la taille des blancs

Sauvegardes

- il faut en faire
- elles doivent être automatisées
- attention à la confidentialité : chiffrement des sauvegardes ?
- penser au vol, à l'incendie, … : sauvegardes hors site
- timemachine (MacOS) : un bon exemple d'outil efficace

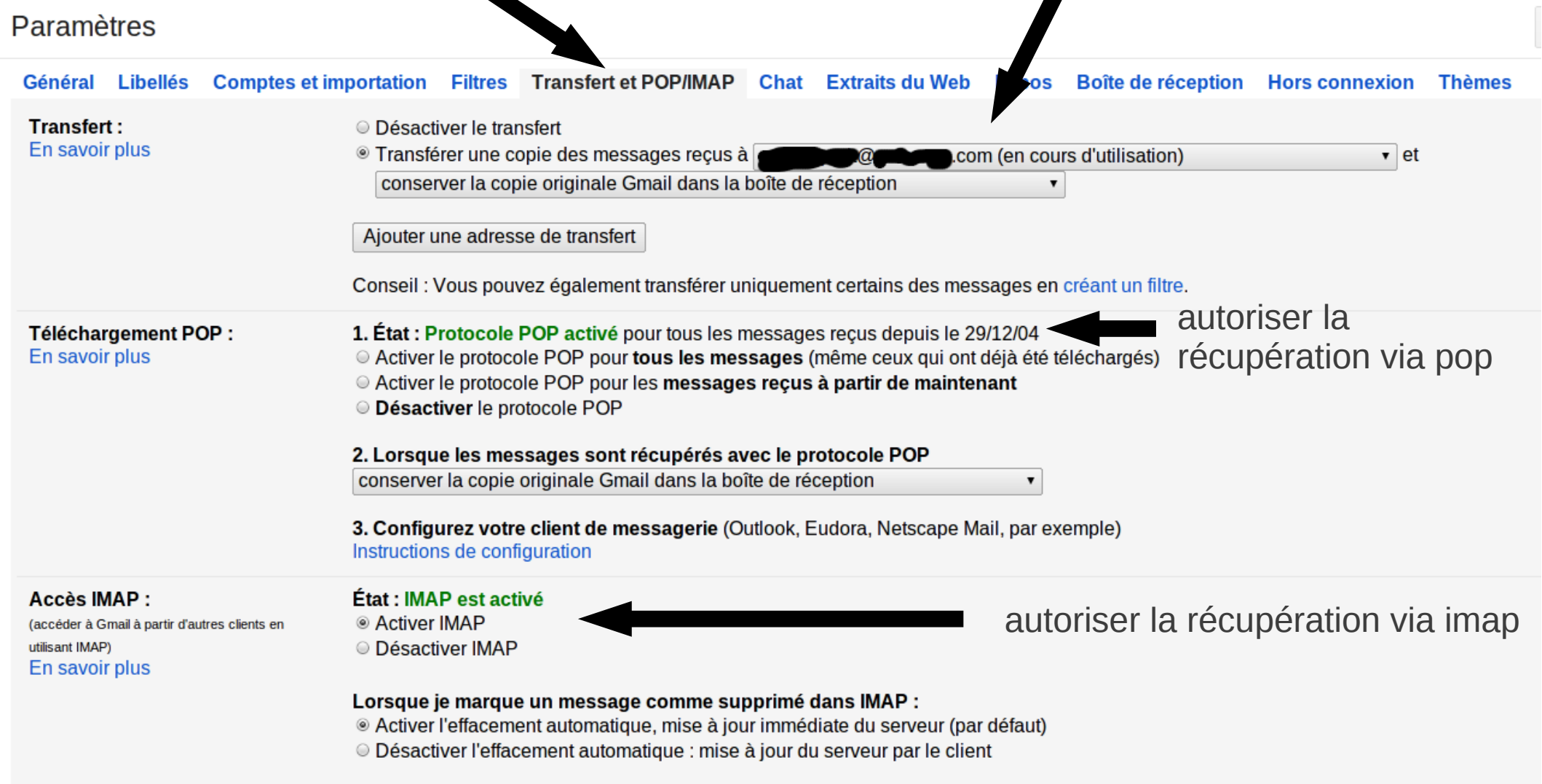
google docs, gmail

- du danger de tout stocker en ligne :
  - http://ehsanakhgari.org/blog/2012-04-14/how-i-lost-access-my-google-account-today
  - en cas de fermeture du compte par le prestataire
    - arrive chez google, facebook, …
  - en cas de perte de données de la part du prestataire
- Solution : google takeout
  - https://www.google.com/takeout/
  - permet de récupérer une grande partie de ses données google
  - à faire de façon régulièrement de préventive
- gmail : solution
  - avoir une copie de ses mails localement via un client lourd
    - via protocole pop (copie locale des mais) : ne récupère pas les dossiers
    - via imap : ATTENTION :
      - à bien parametrer la récupération (et pas l'accès distant en ligne)
      - par défaut, imap permet la consultation des courriers présents sur le serveur
  - avoir une copie de ses mails sur une autre adresse mail (se paramètre via l'interface de goole) : méthode conseillée

Gmail

paramètres transfert
et accès distant

transfert vers un autre
compte



autoriser la
récupération via pop

autoriser la récupération via imap

Quelques notions de sécurité à destination du chercheur non informaticien

Plan

- Sécurité : pourquoi ?
- réseau, wifi
- Certificats, https
- téléphones mobiles
- Protection physique (mot de passe bios, chiffrement du disque dur)
- gestion des mots de passe
- sécurité des portables et du navigateur WeB (principalement orienté sur firefox et chrome : flash, javascript, pdf, …)
- bonnes pratiques (mail, formats de documents) où comment transmettre sans le vouloir des informations confidentielles

Sécurité : pourquoi ?

- Confidentialité de votre travail, de votre messagerie, des coordonnées de vos contacts
- Usurpation : faire des choses illégales en votre nom
- Rebond/botnets : utiliser votre installation informatique sans votre accord
- Ransonware : chantage à la perte de données

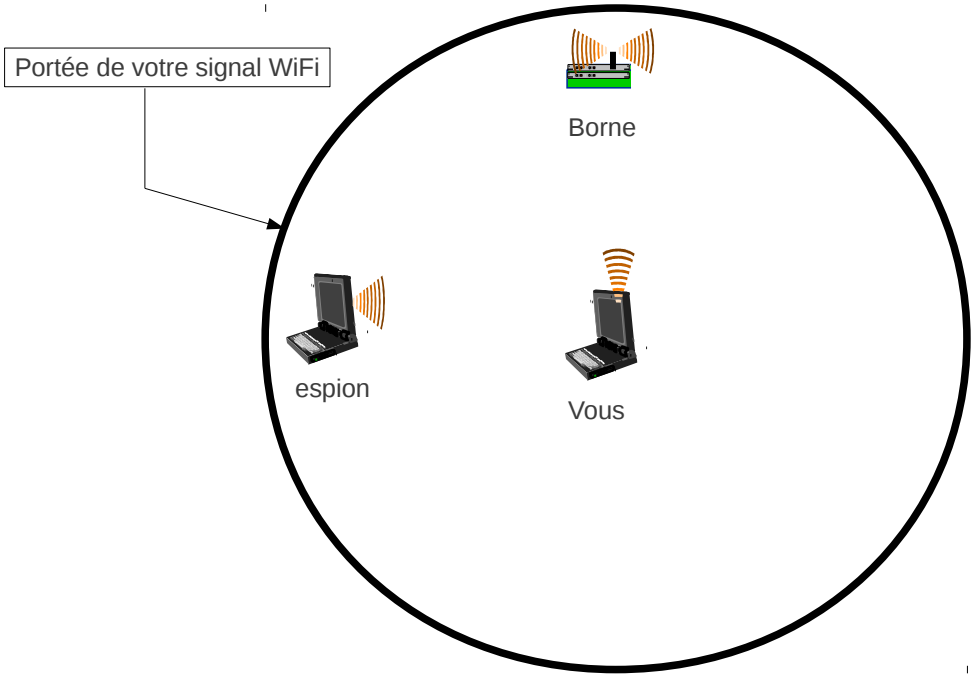
On vit dans un monde formidable !

- Regardons un bulletin du CERT RENATER
- http://sites.univ-provence.fr/wcri/d_serv/d_reseau/d_cert/courant/certmsgSTAT13

WiFi : enjeux

- Utilisation du réseau par un utilisateur non légitime
  - Pour rebond
  - Pour réseau local
  - Pour attaque des autres postes WiFi
    - Solution : interdire les connexions entre postes WiFi (réglage point d'accès)
- Espionnage des données échangées :
  - Sites consultés
  - Mot de passe
  - ...

WiFi : enjeu



WiFi : sécurité

- Ouvert : pas de chiffrement. En général associé à un portail d'authentification
- WEP : chiffrement MAIS cassable en quelques minutes par tout clampin
- WPA1/WPA2 personnal : chiffrement solide (si clef solide) MAIS clef commune
- WPA2 entreprise + 802.1X + méthode génératrice de clef : chiffrement solide, clef unique par poste
- Exemples : google cars.
- Solutions
  - https plutôt que http
  - VPN

Solutions : http/https

- Utiliser https partout où c'est possible
  - Trafic chiffré entre votre navigateur et le serveur
  - Authentification du serveur
- Extension firefox : httpseverywhere (https://www.eff.org/https-everywhere)

Certificats, https

Carte d'identité

Pascal PETIT

Certificats, https

Certificats :

- Un certificat :
  - Identité,
  - clefs publique
  - Certifiés par une autorité de certification
- Permet l'authentification d'un site
  - Le site possède la clef privée associée
  - Le site indiqué par le certificat est bien celui auquel on se connecte
- Permet la mise en place d'un tunnel chiffré : protège contre l'espionnage des communications

certificats et hameçonnage

- Du phishing pour identifier les opposants à Bachar El-Assad
  - faute site youtube annonçant une fausse mise à jour de flash
    - => installation d'un logiciel espion
  - faux site facebook ou youtube
    - récupérer login et mot de passe (y compris des personnes qui mettent des commentaires)
- source : Numerama, 30 mars 2012 :
  http://www.numerama.com/magazine/22197-du-phishing-pour-identifier-les-opposants-a-bachar-el-assad.html

limite de https

- vigilance des utilisateurs (cf exemple syrien)
- fiabilité des autorités de certification
  - que penser d'une AC liée à un pays
  - impact possible
    - créer un faux certificats reconnu comme valide par le navigateur
    - l’hameçonnage sans détection possible
- solutions :
  - aucune
  - une idée : associer les certificats de sociétés connue à des AC et refuser les certificats signés par d'autres AC
  - revient à refuser une carte d'identité d'un français si elle est validée par la Grande Bretagne

smartphones

- des téléphones aux usages variés qui induisent de nouveaux risques
  - photos
  - données (le tel. sert souvent de clef USB)
  - données personnelles
  - accès aux comptes mails & Co via les applications ou les caches locaux
- Les risques
  - vol du téléphone
    - accès aux données présentes dans le tel. (photos, données, ...)
    - accès aux comptes mails & Co depuis le tel.
    - utilisation du téléphone
  - ver, virus & Co
  - application frauduleuse

Vol du téléphone :

- il faut rendre le tel. et ses accessoires (carte mémoire) inexploitables en cas de vol ou d'emprunt
  - code au déverrouillage
  - effacement des données en cas de code incorrect
  - chiffrement des données
  - limiter les données stockées sur le tel.
- récupérer son tel. :
  - installer des applications dédiées (géolocalisation, prise de contrôle à distance, …)
  - exemple : cerberus sous android

Vers/virus & Co

- modèle de sécurité des mobiles
  - limite grandement les problèmes

Applications frauduleuses

- frauduleuses ou pas. Comme le dit l'adage :
  - si le service est gratuit, c'est que vous n'êtes pas le client mais la marchandise
  - cet adage est particulièrement vrai de nos jours :
    - google, facebook
    - les applications gratuites sur mobile ou autre
- applications frauduleuses qui piratent vos données personnelles
- exemples : cf http://www.ecrans.fr/iPhones-beaucoup-trop-d-applis,14100.html
  - l'application ratp
  - twitter,path : tout le carnet d'adresse est collecté

mars 2011 : l'application RAPT

- cf http://www.rfc1149.net/blog/2012/03/20/a-qui-la-ratp-vend-elle-nos-informations-personnelles/
- en résumé : sans avoir prévenu, l'application envoie les informations suivantes à un publiciste :
  - user_position: notre position
  - uphone: +3365970xxxx; le No de tel. complet du tel.
  - imei: 35479504154xxxx; l'imei
  - carrier: votre opérateur
  - ugender, uage, uemail, uzip, unick: non renseignés; heureusement, l'application n'a pas réussi à récupérer les informations de sexe, âge, adresse de messagerie, code postal et pseudonyme.

mars 2011 : l'application RAPT

- comme le signale Samuel Tardieu, l'application RAPT demande des permissions pas forcément déraisonnables :
  - la possibilité de vous localiser : c'est compréhensible pour pouvoir vous guider jusqu'à l'arrêt de transports en commun le plus proche ;
  - l'accès à Internet : indispensable pour récupérer les horaires et les informations à jour ;
  - les informations de contact et l'identité du téléphone : certaines applications les utilisent pour construire un identifiant anonyme, ne permettant pas de vous identifier, mais autorisant le serveur à recouper vos requêtes à des fins statistiques.

téléphone mobile : iphone

- Mac Affee a publié 10 conseils de sécurité pour possesseurs de matériel Apple :
  - cf http://www.mcafee.com/us/resources/white-papers/foundstone/wp-top-10-iphone-security-tips.pdf

téléphone mobile android

- mot de passe au verrouillage
- chiffrer le contenu du tel.
- n'installer que des applications
  - du market/playstore
  - ayant été téléchargées par un nombre important de personnes
  - en vérifiant la cohérence des demandes d'autorisation par rapport aux fonctionnalités
- installer un logiciel de prise de contrôle à distance comme cerberus

Dropbox

- avril 2011 : changement des conditions d'utilisation de dropbox
- avant, dropbox vantait la qualité de son chiffrement AES 256bits
- détection de doublon
  - pour gagner de la place
  - suppose que dropbox puisse déchiffrer les fichiers chiffrés
- BIBLIO :
  - http://www.cnetfrance.fr/news/dropbox-induisait-en-erreur-sur-la-confidentialite-des-donnees-et-le-cryptage-39760824.htm

Dropbox : solution

- chiffrer les données soit même
- via true crypt :
  - pénible car suppose le transfert de tout le contener à chaque modification
  - soit avec des solutions fichiers par fichiers à la encfs
    - pcimpact : http://www.pcinpact.com/dossier/chiffrement-cloud-encfs-boxcryptor-dropbox/209-1.htm
    - http://korben.info/dropbox-chiffrer-crypter-securiser.html
    - http://korben.info/boxcryptor-dropbox-crypte.html
    -

Protection des disques durs

- Mot de passe du bios
  - Peut être supprimé par un voleur
  - Ne l'utiliser que pour empêcher l'utilisation du portable en votre absence
- Mot de passe du disque dur
  - Le mot de passe est stocké dans l'électronique du disque
  - Beaucoup plus résistant
  - Plusieurs niveaux de sécurité (récupérable par le constructeur ou non)
- Chiffrement de partitions ou de disques

Truecrypt : références

- Le FBI se serait cassé les dents dessus : http://sid.rstack.org/blog/index.php/400-pbkdf2-a-l-epreuve-du-fbi
- Rapport de certification de la version 6.0a : http://esec.fr.sogeti.com/FR/documents/presse/tc_dcssi.pdf
- Site officiel : http://www.truecrypt.org/

True crypt fonctionnalités

- Peut chiffrer un disque virtuel dans un fichier
- Peut chiffrer une partition (y compris la partition où est installé windows)
- Le chiffrement est transparent et automatique
- Permet de la stéganographie (méfiance : des travaux récents permettent de détecter les conteneurs truecrypt)
- Fournit des mécanismes de déni plausible en cas de fourniture forcée du mot de passe

encfs/box cryptor

- outils de chiffrement de dossier
- chiffre fichiers par fichiers
- plus efficace en cas de synchronisation entre dossiers sauvegardés
- les outils :
  - encfs/cryptkeeper : sous linux
  - boxcryptor : sous windows

Chiffrement : ne pas jouer avec les autorités :

- Si vous êtes épicier à Tarnac
- Si vous allez visiter un pays un peu parano
  - Ne pas cacher l'existence de données chiffrées
  - On peut vous obliger à fournir la clef de déchiffrement
  - On peut copier l'intégralité du de votre mobile, de votre portable, …
  - Dans les labos, utilité de prévoir un portable blanc remis à zéro régulièrement et ne servant qu'à ça.
- Références :
  - http://www.dgdr.cnrs.fr/fsd/securite-systemes/documentations_pdf/securite_systemes/consignes-portables-etranger.pdf
  - http://www.numerama.com/magazine/3065-la-douane-americaine-peut-fouiller-votre-disque-dur.html
  - http://www.generation-nt.com/pc-portable-douane-police-actualite-18291.html

Mots de passe

- Mots de passe différents et solides
- Hiérarchiser les mots et les contextes d'utilisation
- Pourquoi ?
  - Attaque par dictionnaire ou par force brute sur une empreinte
  - Site WeB peu scrupuleux
    - exemple de Raymond qui s'est fait piraté son compte gmail pour envoyer du spam
  - Vol de données
    - cf monster en 2009 : http://sid.rstack.org/blog/index.php/319-oops-i-did-it-again)
    - Sony récemment : http://www.ecrans.fr/PlayStation-Network-77-millions-de,12576.html
  - Des impacts différents (gestion de compte bancaire, ...)

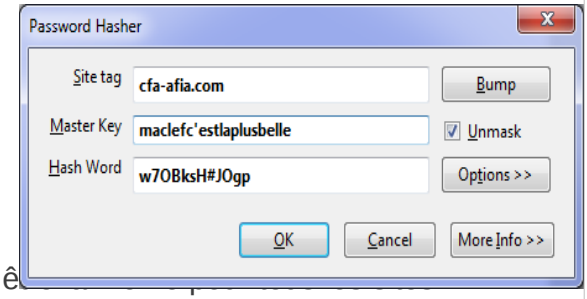
Solution :

- Changer les mots de passe par défaut des logiciels et matériels
- Sinon, vous aurez affaire à Chuck Nouris : http://www.zdnet.fr/actualites/chuck-norris-inflige-une-manchette-aux-modems-dsl-39713237.htm

Solutions : mémorisation des mots de passe par le navigateur

- Pratique
- Le fichier contenant les mots de passe doit être protégé
- Firefox :
  - mot de passe principal de sécurité
  - Sert à chiffrer le fichier contenant les mots de passe
  - il faut en mettre un
- Chrome :
  - Système similaire mais automatique
  - Attention : si on a accès à votre session, les mots de passe sont visibles dans les options de chrome
- Attention : Un attaquant qui a votre mot de passe principal a tous vos mots de passe (keyloger, ...)

Solution : hasher, hash it !



- un mot de passe
  - Différent sur chaque
  - Dépendant
    - Du site (site tag)
    - D'une clef maître qui peut ê
- Des outils compatibles :
  - Hasher pour firefox
  - passwordhasher pour chrome
  - Hash It ! Pour android
- Attention : si un intrus récupère votre mot de passe principal, il peut calculer tous vos mots de passe !

Solution : stockage sécurisé de mots de passe

- 1password
- *keyring
- Problèmes :
  - Niveau de sécurité de l'outil
  - Compromission du mot de passe principal
- Solutions :
  - Stockage sur un autre outil informatique (smartphone?)
  - MAIS gare à la sécurité sur les smartphone

Ransonware :

- Chiffrent fichiers ou disques durs
- Demandent de l'argent pour fournir la clef de déchiffrement
  - Certains sont faibles et facilement contournables
  - Les versions récentes sont très solides
- Une seule solution en cas d'infection :
  - Avoir de bonnes sauvegardes
- Exemple
  - Gpcode analysé dans un article de Nicolas Brulez de la revueMisc No 55 (mai-juin 2011)
  - Utilise de la crypto symétrique et asymétrique solides

Botnets : pourquoi, comment ?

Sécurité du poste de travail

- Impossible
- Des outils grand public qui sont durablement des passoires :
  - Produits adobe (flash, acrobat reader) : des fonctionnalités peu utiles les affaiblissent
  - Navigateurs WeB (internet explorer mais pas que lui)
  - …
- Des systèmes d'exploitation très utilisés et très attaqués
- http/https : pour éviter le sniffage réseau
- difficile de se protéger de l'équipe système qui a les moyens de mettre en place des keyloggers & Co

Solutions : http/https

- Utiliser https partout où c'est possible
- Extension firefox : httpseverywhere (https://www.eff.org/https-everywhere)

Solutions Flash :

- S'en passer:-)
  - Via le support html5 des navigateurs récents : firefox4, chrome, ie9, safari, opera)
  - Problèmes :
    - Les sites consultés doivent supporter html5
      - Youtube : supporte html5 (webM)
      - Dailymotion : supporte html5 (h264)
    - La guerre des codec video : webM (google, firefox, opera) contre H264 (ie9, safari)
  - C'est la meilleure solution mais difficile à vivre (sauf ipad & Co qui n'a pas flash:-))

Solutions Flash :

- Être prudent :
  - Pas de sites pornographiques ! Ou douteux
  - Utilisation d'outils de filtrages :
    - On active ponctuellement flash sur une video de son choix en cliquant dessus
    - Flashblock (chrome, firefox)
    - ClickToFlash (safari)
  - Mise à jour de flash
    - Chrome : intègre flash, garantit une mise à jour rapide
    - Sinon, penser aux mises à jour du Plugin

WeB : éviter les sites douteux : WebOfTrust

- un outil collaboratif
  - l'accès à un site peut être interdit s'il est considéré comme dangereux
  - on peut passer outre l'interdiction
- très facile d'accès
  - devrait être installé par défaut sur les navigateurs
- gare aux abus du collaboratif :
  - à une époque, le site de l'UMP avait été déclaré comme dangereux

WeB : noscript

- N'autorise le javascript que de certaines sources
- Rappel : une page WeB peuplée d'objets de sources variées
- Idéal contre la publicité et certaines formes de flicage
- Un peu lourd à l'utilisation
- Idéal pour la sécurité

Skype

VPN kesako ?

VPN à l'UEVE

Mail & Co : bonnes pratiques

- Mail : gare à la diffusion involontaire d'information
- Informations contenues dans les documents pdf, m$-office & Co

Mail : du danger de la citation

- Guerre de religions avec 2 sectes :
  - Le dinosaures : Ceux qui répondent au dessous du texte cité
  - Ceux qui répondent au dessus du texte cité
  - ràf : un exemple de chaque

Mail : du danger de la citation

- Citer l'intégralité du courrier auquel on répond
- Au fil des échanges, ajouter des destinataires
- => danger
- Exemple : cf ràf
- Bonne pratique :
  - Choisir sa secte (pas important)
  - Relire la partie citée
  - En supprimer les parties non pertinentes du courrier cité

mail : stockage, diffusion

- avoir accès au serveur où sont vos boîtes aux lettres permet de lire vos mails
- toute machine où passent vos mails est un point où ils peuvent être espionnés
- gmail : google analyse le contenu de vos mails pour vous profiler
- conseil : soyez paranoïaques
  - des solutions techniques et des adresses différentes selon les activités (prof. perso, syndicales, …)
  - utilisez le chiffrement des courriers

Faire parler les documents plus qu'ils ne le devraient

- Référence principale : MISC Mag HS No 3, page 40 à 49 : « Faire parler les documents plus qu'ils ne le devraient » de Frédéric Raynal et François Gaspart.
- Plan :
  - Métadonnées
    - Bureautique microsoft
    - Pdf
  - Versions
    - Pdf
    - Microsoft
  - Séparer la forme du fond : exemples à ne pas suivre
    - Cadres noirs en pdf
    - Écriture blanc sur blanc
    - Analyse de la taille des blancs

Sauvegardes

- il faut en faire
- elles doivent être automatisées
- attention à la confidentialité : chiffrement des sauvegardes ?
- penser au vol, à l'incendie, … : sauvegardes hors site
- timemachine (MacOS) : un bon exemple d'outil efficace

google docs, gmail

- du danger de tout stocker en ligne :
  - http://ehsanakhgari.org/blog/2012-04-14/how-i-lost-access-my-google-account-today
  - en cas de fermeture du compte par le prestataire
    - arrive chez google, facebook, …
  - en cas de perte de données de la part du prestataire
- Solution : google takeout
  - https://www.google.com/takeout/
  - permet de récupérer une grande partie de ses données google
  - à faire de façon régulièrement de préventive
- gmail : solution
  - avoir une copie de ses mails localement via un client lourd
    - via protocole pop (copie locale des mais) : ne récupère pas les dossiers
    - via imap : ATTENTION :
      - à bien parametrer la récupération (et pas l'accès distant en ligne)
      - par défaut, imap permet la consultation des courriers présents sur le serveur
  - avoir une copie de ses mails sur une autre adresse mail (se paramètre via l'interface de goole) : méthode conseillée

Gmail


paramètres transfert
et accès distant
transfert vers un autre
compte
Paramètres
Général Libellés Comptes et importation Filtres Transfert et POP/IMAP Chat Extraits du Web os Boîte de réception Hors connexion Thèmes
Transfert :
En savoir plus
Désactiver le transfert
Transférer une copie des messages reçus à [redacted].com (en cours d'utilisation) et
conserver la copie originale Gmail dans la boîte de réception
Ajouter une adresse de transfert
Conseil : Vous pouvez également transférer uniquement certains des messages en créant un filtre.
Téléchargement POP :
En savoir plus
1. État : Protocole POP activé pour tous les messages reçus depuis le 29/12/04
Activer le protocole POP pour tous les messages (même ceux qui ont déjà été téléchargés)
Activer le protocole POP pour les messages reçus à partir de maintenant
Désactiver le protocole POP
autoriser la
récupération via pop
2. Lorsque les messages sont récupérés avec le protocole POP
conserver la copie originale Gmail dans la boîte de réception
3. Configurez votre client de messagerie (Outlook, Eudora, Netscape Mail, par exemple)
Instructions de configuration
Accès IMAP :
(accéder à Gmail à partir d'autres clients en utilisant IMAP)
En savoir plus
État : IMAP est activé
Activer IMAP
Désactiver IMAP
autoriser la récupération via imap
Lorsque je marque un message comme supprimé dans IMAP :
Activer l'effacement automatique, mise à jour immédiate du serveur (par défaut)
Désactiver l'effacement automatique : mise à jour du serveur par le client