Formation au chiffrement des courriels : travaux pratiques

1 Introduction et cours

1.1 Bonnes pratiques en matière de courrier électronique

Cf. « Fiche pratique : sécurité, confidentialité et confort sur Internet », chapitre 2.2.

http://www.ecologielibidinale.org/fr/fiches/tic/miel-fiche-tic-securite-fr.htm#chap2

1.2 Confidentialité des courriels

Cf. « Fiche pratique : confidentialité des courriels ».

http://www.ecologielibidinale.org/fr/fiches/tic/miel-fiche-courriel-fr.htm

2 Travaux pratiques

2.1 Diagnostic technique

2.1.1 Quelle est votre situation actuelle ?

Remplissez le tableau et identifiez dans quel(s) cas vous vous trouvez.

Accès au courriel	**Ordinateur personnel privé connecté à Internet**	**Ordinateur « personnel » chez votre employeur** (dans votre bureau)	**Ordinateur partagé, ressource réseau personnelle** (ex : salle informatique)	**Ordinateur public** (ex : bibliothèque publique, cybercafé)
Outils OpenPGP	Installé =	Installé =	Installé =	(sans objet)
Logiciel de messagerie	Cas 1a Utilisé =	Cas 2a Utilisé =	(sans objet)	(sans objet)
Webmail	Cas 1b Utilisé =	Cas 2b Utilisé =	Cas 3 Utilisé =	Cas 4 Utilisé =

2.1.2 Installation de OpenPGP sur l'ordinateur utilisé pour accéder à Internet

Sous Linux et Mac OS X GnuPG est en principe déjà intégré. Sous Windows : l'outil recommandé est GnuPT (=GnuPG + WinPT).

Cas n°1 : (Windows) installez GnuPT sur votre ordinateur.

Cas n°2 : demandez à l'administrateur de vous installer GnuPG sur votre ordinateur. En cas de refus, vous serez dans le cas n°4.

Cas n°3 : demandez à l'administrateur d'installer GnuPG et FireGPG sur les machines de la salle informatique. Votre trousseau de clé sera lui sur votre ressource réseau personnelle. En cas de refus, vous serez dans le cas n°4.

Cas n°4 : l'ordinateur sur lequel vous vous connectez accepte-t-il les clés USB ?
- Si oui : utilisez une clé USB sur laquelle vous aurez installé une version portable des logiciels nécessaires et compatible avec le système d'exploitation installé (ex : la « framakey Ubuntu »).
- Si non : vous ne pourrez pas chiffrer/déchiffrer vos courriels. Contactez un autre étudiant qui se trouve dans le cas n°1 et qui partagera sa machine avec vous le temps de la formation.

2.1.3 Utilisation d'un logiciel de messagerie : vous êtes dans le cas n°1a ou 2a.

Sous Windows et Mac, le logiciel (libre) recommandé est Thunderbird. Installez son extension Enigmail (interface pour GnuPG). Si vous souhaitez continuer à utiliser un autre logiciel de messagerie, vous devrez installer une interface adéquate.
Les logiciels de messagerie distribués avec Linux intègrent en principe déjà la fonctionnalité.

2.1.4 Utilisation d'un webmail : vous êtes dans le cas 1b, 2b, 3 ou 4.

Vous devez utiliser le logiciel libre Firefox comme navigateur. Installez son extension FireGPG (interface pour GnuPG). Vous pourrez alors effectuer manuellement les actions à l'aide du menu contextuel, après avoir sélectionné le texte.
Cette solution est nettement moins pratique que l'usage d'un logiciel de messagerie où les fonctions seront automatisées.
Dans le cas 4, vous devrez utilisez une version portable du navigateur sur clé USB, si possible.

2.2 Séance n°1

Échange des adresses courriel :

- le formateur donne son adresse ;
- le formateur fait circuler une feuille pour récupérer les noms et adresses courriels de chacun.

Le formateur donne l'empreinte de sa clé publique :

- remise en main propre de sa carte de visite (empreinte) à chaque étudiant : celui qui la reçoit la date et la signe immédiatement.

2.3 Inter-séance n°1 (ou en séance si la salle informatique est correctement équipée)

Le formateur envoi, par courriel, sa clé publique à tous les étudiants.

Chaque étudiant :

- installe sur son ordinateur personnel (ou sur une clé USB), les logiciels nécessaires (cf. § 2.1.) ;
- génère une paire de clé et un certificat de révocation ;
- exporte sa clé publique dans un fichier ascii blindé (.asc) ;
- envoi sa clé publique en pièce jointe au formateur et à tous les étudiants (« répondre à tous » à partir du courriel envoyé par le formateur ;
- prépare une série de carte de visites en y copiant l'empreinte de sa clé publique. Il en imprime autant qu'il y a d'étudiants + une pour le formateur.

Puis :

- importe dans son trousseau de clé chaque clé publique reçue par courriel (celle du formateur et celles de tous les autres étudiants) ;
- vérifie l'empreinte de la clé du formateur à l'aide de la carte de visite que celui-ci lui a remis en main propre. Si l'empreinte correspond, l'étudiant signe la clé du formateur (avec sa propre clé) et lui attribue une validité et un niveau de confiance.

2.4 Séance n°2

Chaque étudiant donne l'empreinte de sa clé publique :

- remise en main propre de sa carte de visite (empreinte) à chaque étudiant et au formateur : celui qui la reçoit la date et la signe immédiatement.

2.5 Inter-séance n°2 (ou en séance si la salle informatique est correctement équipée)

Le formateur et chaque étudiant :

- vérifie l'empreinte de chaque clé à l'aide de la carte de visite que le propriétaire lui a remis en main propre. Si l'empreinte correspond, la personne signe la clé (avec sa propre clé) et lui attribue une validité et un niveau de confiance.

2.6 Tests (exercices)

2.6.1 Test de signature

Le formateur envoi un message signé collectif, incluant une pièce jointe, à tous les étudiants dont il a pu vérifier la validité de la clé publique.
Chaque destinataire en vérifie la signature. Il répond *à tous* par un message signé en précisant s'il a réussi l'opération.

Test à effectuer une fois avec l'option PGP/MIME et une fois sans cette option.

2.6.2 Test de chiffrement

Le formateur envoi un message chiffré *et* signé collectif, incluant une pièce jointe, à tous les étudiants dont il a pu vérifier la validité de la clé publique.
Chaque destinataire déchiffre le message et en vérifie la signature. Il répond *à tous* par un message chiffré et signé en précisant s'il a réussi l'opération.

Test à effectuer une fois avec l'option PGP/MIME et une fois sans cette option.

2.6.3 Test de transfert de courriel avec PGP/MIME

Ici les étudiants sont répartis en groupes de deux.
Pour chaque groupe :

- Le formateur (A) envoi un message chiffré et signé, incluant une pièce jointe, à l'étudiant (B) et lui demandant de transférer le message avec sa pièce jointe, à l'étudiant C, lequel doit ensuite le faire suivre au formateur.
- B transfère le message de façon chiffrée et signée à C.
- C transfère le message de façon chiffrée et signée à A (le formateur).
- A répond à B et C pour leur donner le résultat de l'opération.

2.7 Validation

Le formateur envoi individuellement à chaque étudiant un message chiffré et signé contenant une ou plusieurs question de cours (les questions sont différentes pour chaque étudiant).
Chaque étudiant répond par un message chiffré et signé à la (ou les) question qui lui est posée.
L'évaluation prend en compte la réussite de l'envoi du message et la validité de la réponse à la (ou les) question posée.