Introduction à la cryptographie réseau

Les questions suivantes sont destinées à un premier contact avec la cryptographie appliquée aux réseaux. Elles ne sont pas soumises à évaluation.

Pour les questions portant sur les réseaux, vérifiez vos réponses en utilisant un analyseur de trame (ethereal, tcpdump,...) et en essayant de localiser les informations transmises.

Exercice 1. Authentification et confidentialité. Télécharger la page disponible à l'URL `mail.yahoo.fr`, et visualisez le source de la page.

1. Vérifiez que vous comprenez le javascript et le HTML. Localisez le formulaire de login, le bouton de soumission, le password et le nom du compte.

2. Comment sont transmis le nom de login et le password entre le client (vous) et le serveur. Répondez en comprenant les scripts d'une part et en analysant les trames échangées d'autre part.

3. Qu'est-ce que le MD5 qui aparaît ici ? À quoi sert le `.challenge` ? Que doit mémoriser le serveur ?

4. Quelle est la sécurité ainsi atteinte ?

5. Toujours sur la page de login de yahoo!mail on peut choisir une option de connexion sécurisée. Quel protocole utilise-t'elle ? Regardez le source de la page, où est passé la cryptographie ? Est-ce vraiment plus sûr ?

6. Décrire les échanges de trame dans le cas du login par connexion sécurisée.

Exercice 2. Distribution de clés.

1. Connectez vous à l'interface mèl du CMI : `https://webmail.cmi.univ-mrs.fr/`. Qu'observez-vous ? Quels sont le ou les protocoles utilisés ?

2. Où sont stockés les certificats de votre navigateur ? À quoi servent-ils ? Par quelle méthode obtient-on des certificats ? Est-ce sûr ?

3. La page web de Pascal Weil contient une clé GnuPG. À quoi sert-elle ? Sauriez-vous lui envoyer un message crypté (ne pas le faire) ?

Exercice 3. Fuite d'informations.

1. Comment déterminer de manière simple le type (Apache, IIS, etc.) d'un serveur HTTP ?

2. Comment un serveur Apache protège-t'il certaines pages ?

3. À l'URL `ftp://ftp.cs.rutgers.edu/cs/AcademicIntegrity/private/.htpasswd` on trouve les données suivantes : `instructor:6zo0T7rbLh4OE`

Avez-vous une chance de vous faire passer pour un enseignant d'informatique de l'université de Rutgers ?

4. Où sont stockés les mots de passe d'un système unix ? Où et sous quelle forme étaient-ils stockés autrefois ?

Exercice 4. Regarder le programme `crypt`, comprendre son fonctionnement.