POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

INF4420a: Sécurité Informatique
Cours 6 : Authentification – Exercices – Corrigés

Nora Cuppens

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Question Quiz no. 1

- Choix d'une politique de mots de passe
- Deux politiques vous sont proposées : 1) choisir des mots de passe composés de 6 caractères (lettres minuscules a-z, majuscules A-Z et chiffres 0-9) choisis au hasard et 2) choisir une « phrase » de passe composé de quatre mots du français courant, choisis au hasard. D'un point de vue de sécurité, la première option est plus désirable.

- Réponse : b. Faux

- Pourquoi ?

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Question Quiz no. 1

- Choix d'une phrase de passe (de longueur 4)
  - fraiseiPhonepouletrhododendron

- Choix d'un mot de passe de 6 caractères
  - rZakh1

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Question Quiz no. 1

- Force d'une phrase de passe (de longueur 4)
  - Nombre de combinaisons possibles :
  - Choisir un dictionnaire de 1000 mots
  - 1000^4
  - = 2^40

- Force d'un mot de passe de 6 caractères
  - Nombre de combinaisons possibles :
  - 62^6
  - = 57^9
  - = 2^36

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Question Quiz no. 1

- Est-ce que le choix de la langue de la phrase de passe est important ?

  1. Oui
  2. Non
  3. Ca dépend

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Question Quiz no. 1

- Est-ce que le choix des mots de la phrase de passe est important ?

  1. Oui
  2. Non
  3. Ca dépend

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Question Quiz no. 1

- Est-ce qu'on prend un risque important si on révèle le dictionnaire utilisé pour générer la phrase de passe ?

  1. Oui
  2. Non
  3. Ca dépend

Exercices de crypto

- Question Quiz no. 1

- Est-ce qu'on prend un risque important si on révèle le dictionnaire utilisé pour générer la phrase de passe ?

- Prenons un dictionnaire de 20000 mots
- Ça va engendrer 20000^4 combinaisons possibles
- = 160 * 10^15
- = 2^7 * 2^50
- = 2^**57**
- Même force qu'une clé DES

Exercices de crypto

- Question Quiz no. 7

- Votre ancienne politique de mots de passe forçait vos usagers à utiliser un mot de passe d'exactement 6 caractères alphabétique en minuscules (a-z). Pour renforcer la sécurité, vous demandez maintenant des mots de passe de 8 caractères, pouvant contenir des minuscules, majuscules et chiffres (a-z + A-Z + 0-9). De combien de bits effectifs avez-vous renforcé le mot de passe si on considère que vos usagers choisissent des mots de passe complètement aléatoires ?

- Réponse : b. Augmentation de 19.4 bits effectifs

Exercices de crypto

- Réponse Quiz question 7 :

- Entropie initiale du mot de passe sur 6 caractères
  - Entropie de la source correspondant à chaque caractère :
    - $H(S) = \sum_i p_i \log_2 (1/p_i)$ avec $0 \leq i \leq 25$
    - $H(S) = 26 * 1/26 \log_2 (26) = \log_2 (26)$ (chaque lettre est équiprobable)
    - H(S) = 4,70 bits
  - Entropie de la source correspondant au mot de passe
    - H(S) = 6 * 4,70 = 28,20 bits (source markovienne)
  - Méthode 2
    - Nombre de mots de passe possible 26^6 ≈ 309 * 10^6
    - 2^28 ≤ 309 * 10^6 ≤ 2^29
    - Un mot de passe correspond à une clé entre 28 et 29 bits

Exercices de crypto

- Réponse Quiz question 7 :

- Entropie du mot de passe sur 8 caractères
  - Entropie de la source correspondant à chaque caractère :
    - $H(S) = \log_2 (62)$ (chaque caractère est équiprobable)
    - H(S) = 5,95 bits
  - Entropie de la source correspondant au mot de passe
    - H(S) = 8 * 5,95 = 47,6 bits (source markovienne)
  - Différence avant / après
    - 47,6 – 28,2 = 19,4 bits

Exercices d'authentification

- Exercice 1 : Force d'un mot de passe

- Objectif :
  - Savoir choisir un mot de passe

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices d'authentification

- Exercice 1 : Force d'un mot de passe
- Plusieurs sites possibles pour évaluer la force d'un mot de passe
- Voir par exemple :
  - https://lowe.github.io/tryzxcvbn/
- Question 1 : D'après vous, comment ça marche ?

Exercices d'authentification

- Réponse question 1 : A vous …

Exercices d'authentification

- Réponse question 1 : D'après vous, comment ça marche ?

- Principe de base
  - Repose sur la recherche dans un dictionnaire
  - Plusieurs dictionnaires
  - Dictionnaire multilingue
    - Anglais / Français / Chinois
  - Recherche dans le dictionnaire les « patterns » présents dans le mot de passe
  - Lorsqu'un « pattern » apparait dans plusieurs dictionnaire, le rang le plus bas est retenu

Exercices d'authentification

- Réponse question 1 : D'après vous, comment ça marche ?

- Transformation sur les mots
  - Retrouve les substitutions « classiques »
    - a → @
    - o → 0
    - s → $
    - Etc.
  - Prend en compte les inversions
    - password → dorwssap

Exercices d'authentification

- Réponse question 1 : D'après vous, comment ça marche ?

- Estimation du temps pour casser le mot de passe
  - Dictionnaire → Rapide
  - Force brute → Plus lent
  - Phrase de passe → Beaucoup plus lent
  - Phrase de passe « complexe » → Très coûteux

- Pour plus d'information
  - https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices d'authentification

- Exercice 1 : Force d'un mot de passe

- Question 2 : Est-ce que les résultats vous paraissent fiables ?
  1. Oui
  2. Non

Exercices d'authentification

- Exercice 1 : Force d'un mot de passe

- Réponse question 2 : Oui et non, mais plutôt oui
  - Réaliste pour les attaques par dictionnaire
  - Plus optimiste pour le reste
    - Peu de surcout de temps de calcul pour les substitutions
    - Peu clair comment est calculé le temps de calcul pour la force brute
    - Peu clair comment est calculé le temps de calcul pour les « phrases de passe »

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification

- Objectifs
  - Savoir identifier les avantages et inconvénients des fonctions d'authentification

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 1 : Authentification simple UserId + Mot de Passe tapé au clavier
- Voir par exemple :
  - https://www.rbcroyalbank.com/fr/personal-c.html
- Question 1 : Avantages et risques de cette solution ?

Exercices d'authentification

- Réponse question 1 : A vous …

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification

- Réponse question 1 :
  - Risque d'attaque par force brute si mot de passe de faible entropie
  - Risque d'interception du mot de passe par un keylogger
  - Risque de récupération du mot de passe
    - Phishing, site pirate cloné, social engineering, « post-it »
  - Risque d'attaque contre le fichier des mots de passe
    - Notamment attaques « internes »

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 1 : Authentification simple UserId + Mot de Passe
- Question 2 : Comment limiter les risques de cette solution ?

Exercices d'authentification

- Réponse question 2 : A vous …

- Risque d'attaque par force brute si mot de passe de faible entropie
- Risque d'interception du mot de passe par un keylogger
- Risque de récupération du mot de passe
- Risque d'attaque contre le fichier des mots de passe

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification

- Réponse question 2 :
  - Risque d'attaque par force brute si mot de passe de faible entropie
    - Imposer le choix du mot de passe à l'utilisateur
    - Ne pas laisser l'utilisateur choisir son mot de passe n'importe comment
    - Obliger l'utilisateur à changer son mot de passe régulièrement
    - Limiter le nombre de tentatives infructueuses
  - Risque d'interception du mot de passe par un keylogger
    - Utilisation d'un anti-virus, mais pas solution à 100%
  - Risque de récupération du mot de passe
    - Sensibilisation des utilisateurs
  - Risque d'attaque contre le fichier des mots de passe
    - Limiter l'accès au fichier des mots de passe (voir cours « Autorisation » et « Sécurité OS »)
    - Détection d'anomalies internes (voir cours de « sécurité réseau »)

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 2 : Authentification simple UserId + Mot de Passe cliqué dans une fenêtre
- Voir par exemple :
  - https://www.credit-agricole.fr/
  - Identifiant = 11 chiffres (numéro de compte)
  - Code personnel = 6 chiffres
- On va revenir là-dessus après l'exemple 3

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 3 : Une variante intéressante
- Voir :
  - mobile.free.fr/
  - Identifiant = 8 chiffres
  - Code personnel = 10 caractères choisis par l'opérateur
- Question 3 : Qu'est-ce que vous trouvez bizarre ?

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices d'authentification

Exercices d'authentification

- Réponse question 3 : A vous …

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 3 : Une variante intéressante
- Question 4 : Est-ce que vous trouvez ça pertinent ?
  1. Oui
  2. Non

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification
- Exemple 2 : Authentification simple UserId + Mot de Passe cliqué dans une fenêtre
- Voir par exemple :
  - https://www.credit-agricole.fr/ca-illeetvilaine/banque-privee/acceder-a-mes-comptes.html
  - Identifiant = 11 chiffres (numéro de comptes)
  - Code personnel = 6 chiffres
- Question 5 : Quels sont les risques de cette solution ?

Exercices d'authentification

- Réponse question 5 : A vous …
  - Comparaison avec Exemple 1 (Authentification simple UserId + Mot de Passe)

Risque moins élevé

Risque plus élevé

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification

- Réponse question 5 : Quels sont les risques de cette solution ?
  - Tous les risques identifiés dans l'exemple 1 restent présents dans l'exemple 2 sauf :
  - Différence 1 : Risque d'interception du mot de passe assez faible
    - Protection contre les keyloggers
    - Transmission du mot de passe par https
    - Risque de screen logger
  - Différence 2 : Risque élevé d'attaque par force brute contre le mot de passe
    - Mot de passe sur 6 chiffres = 10^6 possibilités
    - Equivalent à une clé sur 20 bits (ce n'est pas beaucoup)

Exercices d'authentification

- Exercice 2 : Analyse de fonctions d'authentification

- Réponse question 5 (suite) : Quels sont les risques de cette solution ?
  - Risque élevé d'attaque par force brute contre le mot de passe
    - Collecter un grand nombre de numéros de compte (> 10^6)
    - Tester un ou deux mots de passe contre chaque compte
    - Permet de contourner le blocage des comptes au bout de 3 essais
  - Remarque : le compteur d'échec du mot de passe est remis à zéro lorsque l'utilisateur légitime se connecte
    - Ca devient une vulnérabilité qui permet de jouer le scénario d'attaques ci-dessus plusieurs fois

Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle

- Objectifs
  - Comprendre le concept d'authentification contextuelle
  - Savoir utiliser ce concept

Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle

- Retour sur l'exemple 2 de l'exercice 2
  - Supposons que le mot de passe d'un client de la banque soit cassé

- Question 1 : Est-ce que c'est « game over » pour ce client ?
  1. Oui
  2. Non

Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle

- Retour sur l'exemple 2 de l'exercice 2
  - Supposons que le mot de passe d'un client de la banque soit cassé

- Réponse question 1 : La réponse est non !
  - Plus précisément, c'est « game over » pour la confidentialité de ses comptes
  - Mais pas pour leur intégrité

- Question 2 : Pourquoi ?

Exercices d'authentification

- Réponse question 2 : A vous …

Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle

- Réponse question 2 : Parce que la banque a défini une politique d'authentification contextuelle

- Certaines opérations présentent un risque considéré comme faible
  - Consultation des comptes par le client
  - Les transferts vers les comptes du client

- Certaines opérations ont un risque élevé
  - Par exemple, transfert vers un compte qui n'appartient pas au client

Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle

- Réponse question 2 : Définition de la politique d'authentification contextuelle

  – Avec une authentification simple (Id du compte + Mot de passe), les opérations à risque faible sont permises

  – Pour réaliser une opération à risque élevée, une authentification forte est obligatoire (par Remote One Time Password via le téléphone cellulaire)

Exercices d'authentification

- Exercice 3 : Politique d'authentification contextuelle
- Conclusion Exercice 3

- Conclusion 1 : Si le mot de passe d'un utilisateur est cassé
  - La confidentialité des comptes du client est perdue
  - L'intégrité des comptes du client peut être attaquée
  - Mais l'attaquant ne peut pas vider les comptes du client
- Conclusion 2 : La politique d'authentification peut être beaucoup plus élaborée et dépendre par exemple :
  - De l'environnement (de l'heure, de la localisation du client, etc.)
  - D'une mise à jour du profil du client (changement d'adresse ou de numéro de téléphone cellulaire)
  - Etc.