Année 2012-2013 1ère session

IPB
ENSEIRB MATMECA BORDEAUX

Sécurité des Systèmes d'Information
IT 218
Paul Dorbec

Filière : Informatique Année : 2ième Semestre : S4

Date de l'examen : 29 mai 2013 Durée de l'examen : 2h

Documents autorisés ☒ sans document ☐
Calculatrice autorisée ☐ non autorisée ☒

Autre : Le sujet comporte 2 pages. Il est composé de 3 exercices indépendants, qui peuvent être traités dans un ordre quelconque, et dont les questions sont plus ou moins indépendantes. Le barème est donné à titre indicatif.

SUJET

1 Menaces sur les bases de données

Selon un rapport de Imperva, la menace principale sur les bases de données est l'abus de privilèges excessifs.

Question 1.1 (2pt)
Rappelez le principe du moindre privilège.

Question 1.2 (2pt)
Décrivez un exemple de situation où un utilisateur de base de données pourrait abuser de droits excessifs sur une base de données.

Question 1.3 (2pt)
La deuxième menace du rapport est l'abus de privilèges légitimes. Expliquez en quoi simplement copier localement les données de la base auxquelles on a accès peut présenter un risque.

Question 1.4 (2pt)
Décrivez au moins deux autres menaces que vous pouvez imaginer sur les bases de données.

2 Un peu d'analyse de protocole

Voici un protocole de base, où Alice envoie un message M à Bob. On note N_B un nombre aléatoire généré par B et K_a la clé privée de Alice, dont Bob connaît la clé publique. On note $h(x)$ le résultat de l'exécution d'une fonction de hachage sur un message x.

1. $A \longrightarrow B$: M, A
2. $B \longrightarrow A$: N_B
3. $A \longrightarrow B$: $\{h(M, B, N_B)\}_{K_a}$

Question 2.1 (2pt)
Expliquez l'objectif de ce protocole.

Question 2.2 (2pt)
Expliquez le rôle de l'utilisation d'une fonction de hachage h.

Question 2.3 (2pt)
Expliquez le rôle de l'utilisation du nombre aléatoire N_B. Décrivez des circonstances où une attaque possible sur un protocole sans ce nombre est utile.

3 Authentification et twitter.

Voici un extrait de PC world, 26 mai 2013: http://www.pcworld.com/article/2039753/twitters-stronger-security-isnt-bulletproof-experts-warn.html (la bonne compréhension de l'extrait n'est pas importante pour répondre aux questions).

> While experts praise Twitter's decision to provide account holders with two-factor authentication, they warn that additional security will still be needed to prevent the hijacking of high-profile accounts.
>
> Twitter said last week that people who opt to take advantage of the service will be prompted to enter a six-digit code texted to their mobile phone each time they log into the microblogging service. While such additional authentication is a bit more work, it increases the difficulty for hackers.
>
> Twitter launched the service after a string of account hijackings. Since last month, a group calling itself the Syrian Electronic Army has taken credit for breaking into the accounts of the Associated Press, the Financial Times, National Public Radio and The Guardian. The group says it targets news media that are sympathetic to Syria's rebels.
>
> The AP hack was particularly dramatic. The attackers posted false tweets saying there had been two explosions in the White House, and that President Barack Obama was injured. The bogus report to AP's 1.9 million followers caused the Dow Jones Industrial Average to drop more than 100 points before quickly recovering to erase the losses.

Question 3.1 (2pt)
L'article souligne la mise en place d'une authentification à deux facteurs, d'abord connexion puis confirmation par la requête d'un code à six chiffres envoyé sur le téléphone portable. Expliquez l'intérêt de la mesure.

Question 3.2 (2pt)
Un peu plus loin dans l'article (non cité ici), des experts de la sécurité regrettent que cette authentification double soit facultative. Qu'en pensez-vous?

Question 3.3 (2pt)
Il est aussi signalé que la technique est vulnérable à une attaque "Man in the middle", en imitant la page de connexion de Twitter. Rappelez le principe de cette attaque. Expliquez notamment pourquoi il s'agit d'une attaque "Man in the middle" et non d'un vol d'identifiants classique.