ISEC-AFTI, 2019-20

Examen 20/05/2020

Partie Introduction à la sécurité, J. Leneutre

Exercice 1 : Protocole KSL

Le protocole KSL[1] est un protocole conçu in initialement comme une amélioration du protocole Kerberos V5. KLS utilise de la cryptographie symétrique et fait appel à un serveur. Il a pour objectifs :

1. la distribution d'une clef de session,
2. la distribution d'un « ticket » permettant une authentification mutuelle répétée.

Les hypothèses sont les suivantes :

- `Kas` (resp. `Kbs`) est une clef symétrique long terme (pré-partagée) connue uniquement de A et de S (resp. de B et de S),
- `Kab` est une clef symétrique de session (générée à chaque exécution du protocole KSL),
- `Kbb` est une clef symétrique à court terme connue seulement de B (générée à chaque exécution du protocole KSL),
- `Ra, Rb` et `Rc, Na et Nb` sont des nombres pseudo-aléatoires,
- `Tb` est une *estampille généralisée*, constituée d'une estampille générée par l'horloge locale de B, d'une durée de vie du ticket (relative à l'horloge de B) et d'un identifiant d'horloge (i.e. un nonce qui est mis à jour à chaque fois que l'horloge de B est corrigée).

Les messages du protocole sont les suivants :

1. A --> B : Ra, A

2. B --> S : Ra, A, Rb, B

3. S --> B : $\{Rb, A, Kab\}_{Kbs}$, $\{Ra, B, Kab\}_{Kas}$

4. B --> A : $\{Ra, B, Kab\}_{Kas}$, $\{Tb, A, Kab\}_{Kbb}$, Rc, $\{Ra\}_{Kab}$

5. A --> B : $\{Rc\}_{Kab}$

6. A --> B : Na, $\{Tb, A, Kab\}_{Kbb}$

7. B --> A : Nb,$\{Na\}_{Kab}$

8. A --> B : $\{Nb\}_{Kab}$

Les messages 1 à 5 permettent la génération et l'échange de la clef de session Kab. Les messages 6 à 8 permettent l'authentification mutuelle entre A et B, et peuvent être répétés jusqu'à ce que le ticket $\{Tb, A, Kab\}_{Kbb}$ expire (i.e. jusqu'à ce que *Tb* ne soit plus valide).

1. Montrer qu'il existe une attaque sur la partie concernant l'authentification répétée du protocole (messages 6 à 8), où un attaquant X peut se faire passer pour A auprès de B (sans pour autant connaître Kab) suivant le squelette ci-dessous :

6. X/A --> B : ...

7. B --> X/A : ...

6'. X/A --> B : ...

7'. B --> X/A : ...

8. X/A --> B : ...

---

[1] Axel Kehne, Jürgen Schönwälder, and Horst Langendörfer. Multiple authentications with a nonce-based protocol using generalized timestamps. In *Proc. ICCC '92*, Genua, 1992.

2. Montrer en complétant le squelette ci-dessous, qu'un attaquant X peut faire en sorte que deux tickets générés par deux entités différentes contiennent la même clef de session Kab :

1. X/A --> B : ...

2. B --> X/S : ...

1'. X/B --> A : ...

2'. A --> S : ...

3'. S --> A : ...

4'. A --> X/B : ...

3. X/S --> B : ...

4. B --> X/A : ...

3. Montrer que dans le scénario de la question 3, l'attaquant X peut compléter les message 5 des deux sessions en supposant que X puisse auparavant entamer la phase d'authentification répétée.

4. Commenter les corrections apportées par G. Lowe dans la version modifiée du protocole KSL ci-dessous :

1. A --> B : Ra, A

2. B --> S : Ra, A, Rb, B

3. S --> B : $\{A, Rb, Kab\}_{Kbs}$, $\{Ra, B, Kab\}_{Kas}$

4. B --> A : $\{Ra, B, Kab\}_{Kas}$, $\{Tb, A, Kab\}_{Kbb}$, Rc, $\{B, Ra\}_{Kab}$

5. A --> B : $\{Rc\}_{Kab}$

6. A --> B : Na, $\{Tb, A, Kab\}_{Kbb}$

7. B --> A : Nb,$\{Na, B\}_{Kab}$

8. A --> B : $\{A, Nb\}_{Kab}$

Exercice 2 : Extension du modèle de Bell LaPadula pour l'intégrité

On considère dans cet exercice une extension du *modèle classique de Bell LaPadula* due à R. Sandhu afin de combiner confidentialité et intégrité. Nous appellerons cette extension *modèle étendu de Bell LaPadula pour l'intégrité*.

Les modifications introduites dans le *modèle étendu de Bell LaPadula pour l'intégrité* sont les suivantes :

- on considère un treillis de labels de confidentialité et un treillis de labels d'intégrité ; un label de confidentialité sera noté L_c (ou L_c'), tandis qu'un label d'intégrité sera noté L_i (ou L_i') ; la relation *domine* sera désignée par ;
- on associe à chaque sujet et objet, un couple de label (L_c, L_i) ;
- on considère les deux règles suivantes :
  - (R1) : *un sujet s de label* (L_c, L_i) *peut accéder en lecture à un objet de label* (L_c', L_i') *si* $L_c \geq L_c'$ *et* $L_i' \geq L_i$
  - (R2) : *un sujet s de label* (L_c, L_i) *peut accéder en écriture (seulement) à un objet de label* (L_c', L_i') *si* $L_c' \geq L_c$ *et* $L_i \geq L_i'$

Pour rappel le *modèle classique de Bell LaPadula*, désigne le modèle suivant :

- on considère un treillis de labels de confidentialité ; la relation *domine* sera désignée par $\geq$;
- on associe à chaque sujet et objet, un unique label L;
- on considère les deux règles suivantes :
  - (sécurité simple) : *un sujet de label L, peut accéder en lecture à un objet de label L' si* $L \geq L'$

- (confinement) : *un sujet de label L peut accéder en écriture (seulement) à un objet de label L' si L' ≥ L*

3. On considère deux labels de confidentialité L_c et L_c' tels que $L_c > L_c'$ et deux labels d'intégrité L_i et L_i' tels que $L_i > L_i'$. On note r (resp. w_{-r}) le droit d'accès correspondant à une opération de lecture (resp. écriture seulement). En considérant les droits précédents, et tous les couples possibles de labels de confidentialité et d'intégrité pour les sujets et les objets, construire la matrice des accès autorisés.

4. On considère deux sujets *s* et *s'*, et deux objets *o* et *o'*, ainsi que la matrice de contrôle d'accès suivante :

	o	**o'**
s		r, w_{-r}
s'	r, w_{-r}	r

   a. Montrez qu'il n'existe pas de treillis de labels de confidentialité et une affectation de ces labels aux sujets et objets, tels que les accès autorisés suivant les règles *modèle classique de Bell LaPadula* correspondent à ceux indiqués dans la matrice ci-dessus ? (justifiez)

   b. Peut-on trouver un treillis de labels de confidentialité et un treillis de label d'intégrité et une affectation de couples de labels aux sujets et objets, tels que les accès autorisés suivant les règles du *modèle étendu de Bell LaPadula pour l'intégrité* correspondent à ceux indiqués dans la matrice ? (justifiez)