Informatique et Confidentialité
Exercices - Fiche 1

M1 MEEF parcours NSI 2022-2023

Authentifications simples embarquées

Le but de cet exercice est d'étudier plusieurs scénarios d'identification simple dans le cas des systèmes embarqués et de voir quelles attaques et quelles amélioriations on peut proposer.

Le fait que le système soit embarqué implique que les communications sont difficiles, notamment en ce qui concerne le partage de secret.

1. Cas d'étude : les clefs électroniques permettant d'ouvrir une voiture à distance. Les premières implantations dans les années 90 consistaient juste à envoyer un mot de passe sur 16 bits.
   - Si l'on a un système qui permet d'énumérer tous les codes combien à un rythme de 10 par secondes quel temps faut il en moyenne pour casser le système ?
   - Pourquoi est-ce que même si on passe à 32 bits un système d'identitification basé sur ce schéma n'est pas sûr ?
   - Une amélioriation est de proposer le protocole suivant : la voiture et la clef partagent k, la clef envoie le message $C, \{C, N\}_k$ à la voiture, où C est le numéro de la clef, N un nombre aléatoire et où $\{M\}_k$ dénote le cryptage du message M par la clef k. La voiture décrypte le message et vérifie qu'il est bien constitué. Quelle est la principale faiblesse de ce protocole ?
2. Le protocole IFF (Identification Friend or Foe) est utilisé pour repérer sur les écrans radars quels sont les avions amis des avions ennemis. Pour cela le radar envoie un challenge à l'avion sous la forme d'un nombre aléatoire $\{N\}$ et l'avion doit répondre $\{N\}_k$. Supposez que vous possédez des radars permettant de repérer et de challenger les avions ennemis. Comment pouvez vous les utiliser pour contourner le protocole IFF de l'ennemi ?
3. Quel autre problème de discrétion pose le protocole IFF quand on sait que les retours radars sont plus faibles que celui des émetteurs IFF ?
4. Les premières générations de décodeurs TV possédaient des cartes à puces permettant de décrypter les signaux vidéos en engendrant des clefs (typiquement une dizaines par seconde) en appliquant une fonction cryptographique à certaines informations de contrôle ajoutées au signal vidéo. Imaginez une attaque possible s'il n'y a qu'un seul codage possible pour tous les décodeurs.

One Time Password

Décrivez un système/protocole permettant à une personne de s'identifier auprès d'un vérificateur d'identité (qui peut être une personne ou n'importe quel système informatique) par un mot de passe de telle manière à ce que chaque mot de passe ne soit utilisé qu'une et une seule fois. Le but est de ne pas conserver la liste des mots de passe sur le serveur qui contrôle les mots de passe (sinon il serait possible de le craquer).

On pourra utiliser une fonction à sens-unique f (c'est à dire une fonction pour laquelle il est impossible de calculer x à partir de la connaissance de $f(x)$).

Tout ou rien

Le but est d'étudier un protocole permettant à Alice de vendre des secrets de telle manière à ce qu'elle ne sache pas quel secret elle a vendu et d'autre part que l'acheteur ne connaisse strictement pas plus d'un secret. Pour cela nous donnons un protocole où deux acheteurs, Bob et Carole cherchent à acheter un secret. Nous ajoutons en plus comme contrainte que ni Bob ni Carole ne doit savoir quel secret l'autre acheteur a choisi.

Nous commençons par définir le **FBI** (Fixed Bit Index) de deux suites de bits de même taille. Si ces suites sont x et y alors le **FBI** de x et y est l'ensemble des indices i des bits pour lesquels le ième bit de x est égal au ième bit de y. Les bits se lisant de droite à gauche en commençant par 0. Par exemple :

$$\begin{aligned} x &= 110101001011 \\ y &= 101010000110 \\ FBI(x,y) &= \{1,4,5,11\} \end{aligned}$$

Dans le protocole que nous décrivons Alice est le vendeur, Bob et Carole sont les acheteurs. Alice possède k secrets de n-bits $S_1, S_2, \ldots, S_k$. Bob veut acheter le secret S_b et Carole veut acheter le secret S_c.

1. Alice engendre deux paires de clefs publiques/privées. Une paire est K_B, K_B^{-1} et l'autre est K_C, K_C^{-1}. Alice communique K_B (la clef publique) à Bob (mais pas à Carole) et K_C à Carole (mais pas à Bob).

2. Bob engendre k chiffres aléatoires de n-bits notés $B_1, \ldots, B_k$. Il envoie les B_i à Carole. Carole fait de même : elle engendre $C_1, \ldots, C_k$ et les envoie à Bob.

3. Bob encrypte C_b avec K_B ce qui donne $K_b(C_b)$. Bob calcule le **FBI** de C_b et $K_b(C_b)$ et l'envoie à Carole. Symétriquement Carole encrypte B_c avec K_C et envoie le **FBI** de B_c et $K_C(B_c)$ à Bob.

4. Pour chaque nombre de n-bits $B_1, \ldots, B_k$ il remplace les bits dont l'indice est dans le **FBI** calculé par Carole par son complémentaire (son opposé). Cela produit les nombres $B'_1, \ldots, B'_k$. Il les envoie à Alice.

   Symétriquement pour chaque nombre de n-bits $C_1, \ldots, C_k$, Alice remplace les bits dont l'indice est dans le **FBI** calculé par Bob par son complémentaire (son opposé). Cela produit les nombres $C'_1, \ldots, C'_k$. Elle les envoie à Alice.

5. Alice décrypte les C'_i avec la clef privée associée à Bob. On note $K_B^{-1}(C'_i) = C''_i$. Ensuite Alice calcule $S_i \oplus C''_i$ (où $\oplus$ est le xor bit-à-bit) et envoie le résultat à Bob.

   De même Alice décrypte les B'_i avec la clef privée associée à Carole. On note $K_C^{-1}(B'_i) = B''_i$. Ensuite Alice calcule $S_i oplus B''_i$ (où $\oplus$ est le xor bit-à-bit) et envoie le résultat à Carole.

6. Bob calcule S_b en calculant le xor de C_b et de C'''_b, de son côté Carole calcule S_C en faisant le xor de B_C et de B'''_C

Questions :

- Donnez des exemples d'utilisation de ce protocole. En quoi distribuer des secrets de cette manière peut être utile ?
- Expliquez pourquoi le protocole est correct : pourquoi Bob et Carole trouvent ils le secret qu'ils voulaient acheter ? Pourquoi ils n'apprennent rien d'autre que le secret qu'ils ont acheté (en admettant que tout le monde est honnête) ? Pourquoi est ce qu'Alice ne sait pas quels secrets ont été dévoilé à Bob et à Carole ? Pourquoi est ce que Bob ne connait pas le secret de Carole (et inversement) ?
- Si Alice et Carole ne sont pas honnêtes comment peuvent elles déduire le secret que Bob achète ?