- Défi SEC&SI -

Objectifs, organisation pratique et fonctionnement du défi

ANR, 04 juillet 2008

Objectifs du défi

- Développer un poste sécurisé et cloisonné pour l'internaute.
- Plusieurs contraintes en entrée:
  - Respect du calendrier (phases de développement, phases d'évaluation).
  - Utilisation de composants précis:
    - Machines munies d'un processeur x86.
    - Système d'exploitation sur base Linux.

- Le défi SEC&SI est le premier appel à projet ANR du genre.
  - De ce fait, il aura un caractère expérimental.
  - Les « règles du jeu » pourront évoluer en cours de route avec l'accord de chacun des participants, du jury et de l'ANR.

Périmètre du poste et contraintes

- Le poste doit permettre :
  - Une gestion sécurisée de clefs privées/publiques pour la signature de messages (courriels).
  - Une utilisation sécurisée de services tels que le service de télé- déclaration des impôts.
  - L'utilisation des protocoles SSL/TLS.
  - La sécurisation des données locales.
  - L'utilisation de mise à jour sécurisées.
- En gardant à l'esprit les objectifs:
  - D'ergonomie.
  - D'évolutivité, d'adaptabilité et de portabilité.

Objectifs calendaires

- Structure calendaire rappelée par Vincent Brunie:
  - Successions de phases de développement et d'évaluation.
  - Points d'avancement réguliers des projets.
- Premiers points d'avancement (à confirmer):
  - Première présentation des objectifs des projets et des voies explorées durant les journées C&ESAR 2008 (2-4 décembre 2008).
  - Lancement de la phase d'évaluation après une présentation des projets lors du SSTIC 2009 (juin 2009).

Organisation pratique

- Chaque projet devra (au minimum) être hébergé sur la forge adullact
  - https://adullact.net
- Un projet « SECSI » a d'ores et déjà été créé.
  - Chacun des membres du jury, les coordinateurs et les membres des projets qui le souhaitent pourront s'enregistrer sur la forge et avoir accès au projet « SEC-SI ».
  - Les forums (et les listes de diffusions) pourront être utilisées pour d'éventuels échanges avec le jury ou entre projets et les communications du jury.
- Une procédure particulière sera à respecter pour la mise en évidence de vulnérabilités.

Phase d'évaluation: signaler des vulnérabilités au jury

- Utilisation de GPG (ou équivalent).
- Les vulnérabilités devront toujours être remontées au CERTA (http://www.certa.ssi.gouv.fr) en premier lieu.
    - Ainsi qu'à l'équipe concernée.
    - Et aux éventuels développeurs d'applications ou systèmes impactés.
- Le CERTA transmettra ensuite les éléments techniques au jury qui en concertation proposera une note pour l'attaque.
- Cette note permettra de faire évoluer le score de chacune des équipes.
    - L'équipe qui a découvert l'attaque voit son score augmenter de la note associée à l'attaque. La ou les équipes impactées voient leur score diminuer de la note associée à l'attaque.

Phase d'évaluation

- Les seules attaques autorisées sont les attaques logiques qui ciblent une des solutions.
    - Pas d'attaques sur les serveurs distants.
    - Pas d'attaques physiques sur le matériel des plateformes ou d'attaques de type espionnage (sauf logique).
- Les attaques peuvent être:
    - Soient réelles (preuve de concept).
    - Soit théoriques (supposer l'existence d'une vulnérabilité de tel ou tel composant, supposer que l'attaquant a à sa disposition un réseau de robot par exemple).
- Les attaques réelles auront une note plus élevée que les attaques théoriques.

Evaluation de la pertinence des attaques

- Note de l'attaque en fonction des biens compromis:
  - Biens utilisateur locaux.
  - Biens utilisateur échangés.
  - Matériel cryptographique (clefs).
  - Mises à jour.
- Et des objectifs de sécurité mis en défaut:
  - Confidentialité.
  - Disponibilité.
  - Intégrité.
- Maximum 4 points sont décomptés par bien et par objectif.

Exemple

- Une vulnérabilité du navigateur utilisé par une solution permet d'obtenir un accès à un bien sensible échangé (numéro de compte bancaire). L'architecture du poste permet de limiter l'impact aux seuls biens échangés.

Biens	Confidentialité	Intégrité	Disponibilité
Clefs cryptographiques	0	0	0
Biens échangés	4	2	1
Biens locaux	0	0	0
Mises à jour	0	0	0
Total	4	2	1

- Soit un total de 7 points.

Premier ministre
Secrétariat général de la défense nationale

Coefficient multiplicateur

Type d'attaque	Coeff.	Commentaire
ciblée	1	L'attaque doit viser un internaute particulier. Elle nécessite, par exemple, que son matériel soit vulnérable à une attaque particulière. Dans ce cas il n'y a pas d'aggravation.
générique	2	L'attaque peut être appliquée à tout internaute qui utiliserait cette solution. Par exemple, une vulnérabilité logicielle de la solution est exploitable par un virus. Dans ce cas l'impact est doublé.
systématique	4	L'attaque a un impact immédiat sur tous les internautes utilisant la solution. Par exemple, le système de mise à jour est percé ou une clé de sécurisation du système est compromise.
théorique	¼	Une attaque peut être démontrée moyennant des hypothèses de capacités d'attaque réalistes mais difficiles à mettre en œuvre (disponibilité d'un botnet, de capacité mémoire importante, etc.) ou de vulnérabilité réalistes sur certains composants du système : - le navigateur web ; - le client de messagerie ; - une librairie partagée ; - etc. Dans ce cas, un coefficient réducteur est appliqué. Le fait que ce coefficient ne soit pas nul encourage à publier toute vulnérabilité structurelle et à corriger ces faiblesses avant qu'elles ne deviennent exploitables.

Exemple

- Une vulnérabilité du navigateur utilisé par une solution permet d'obtenir un accès à un bien sensible échangé (numéro de compte bancaire). L'impact est systématique.

Biens	Confidentialité	Intégrité	Disponibilité
Clefs cryptographiques	0	0	0
Biens échangés	4	2	1
Biens locaux	0	0	0
Mises à jour	0	0	0
Total	4	2	1
Impact systématique	16	8	4

- La note pour l'attaque sera de 28 points.

Vulnérabilités mises en évidence par un non participant

- Les projets étant publics, il est possible que des entités non participantes mettent en évidence des vulnérabilités de l'une des solutions.
    - Le jury (ou l'un de ses membres) peut par exemple mener lui même une évaluation des solutions.
    - Des stages peuvent également être lancés sur le sujet.
- Si toutes les solutions sont impactées, leur score n'est pas modifié.
- Dans le cas contraire, la note de l'attaque est retirée au score de chacune des solutions impactées.

Communication sur les projets

- Les différents projets restent maîtres de leur communication.
  - Présentations effectuées, articles publiés, publicité autour du projet, développement d'un site internet du projet.
- Mais il leur sera objectivement nécessaire de communiquer avec le jury notamment dans les phases d'évaluation
  - Pour signaler les corrections apportées en réponse à une vulnérabilité identifiée.
  - Pour signaler une vulnérabilité sur une solution concurrente.