Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE

MINISTÈRE DE LA COHÉSION DES TERRITOIRES

Examen professionnel de vérification d'aptitude aux fonctions de programmeur système d'exploitation

- Session 2018 -

Épreuve écrite n°1
INFORMATIQUE

Composition sur un sujet relatif aux principes généraux du logiciel

Durée : 2 heures
Coefficient : 2
Notation : sur 20
Nombre de pages du sujet : 4 (y compris cette page)

Matériel :
Aucun matériel autorisé.

Documents :
Aucun document autorisé.

Observations :
Il sera tenu compte de la lisibilité et de la propreté des copies, ainsi que de la qualité de l'expression écrite.

Remarques générales :

- Le sujet comporte quatre parties traitant des thématiques suivantes :
  - les systèmes d'exploitation
  - acronymes à définir
  - réseau
  - sécurité

1- Systèmes d'Exploitation (5 points)

A. Mécanismes de communication inter-processus

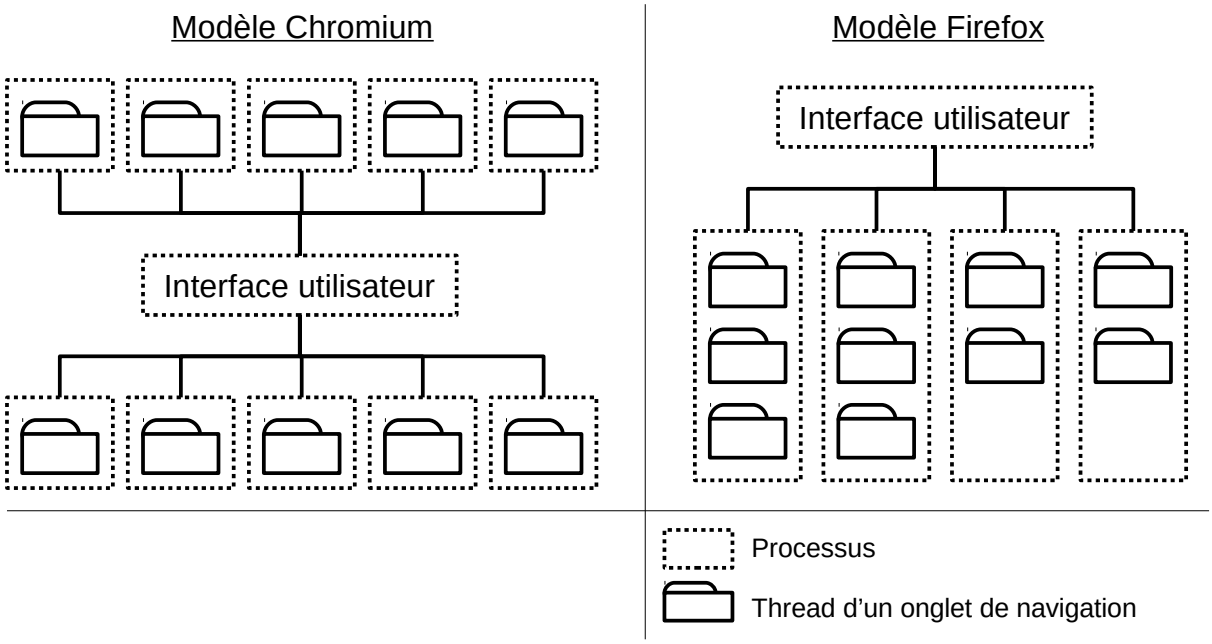
Présentez au moins 4 mécanismes de communication inter-processus.

Pour chaque mécanisme, donnez un exemple de contexte d'application.

B. Processus et processus légers

Expliquez la différence entre un processus et un processus léger (*thread*).

Les dernières versions des navigateurs web ont adopté une architecture multi-processus. Le diagramme ci-dessous montre deux choix d'architecture distincts.



Donnez plusieurs avantages d'une architecture multi-processus pour un navigateur web.

Comparez les avantages et inconvénients des deux modèles d'architecture.

2- Définitions (2 points)

Définissez les acronymes suivants (quelques lignes par acronyme) :

- CSRF
- SDN
- CLI
- API
- DevOps
- Social engineering
- SPF
- CAA

3- Réseau (6 points)

1. Que veulent dire les sigles SSL et TLS ?
2. Expliquer à quoi sert SSL/TLS.
3. Donner deux exemples de protocoles utilisant TLS.
4. Dans la suite de chiffrement TLS_DH_RSA_WITH_AES_128_CBC_SHA, expliquer les différents sigles.
5. En admettant que le serveur est en capacité d'utiliser les deux suites de chiffrement, quelle est la suite de chiffrement que le serveur choisira entre TLS_DH_RSA_WITH_AES_128_CBC_SHA et TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA ? Expliquer ce choix.
6. Comment fonctionne *SNI* et qu'apporte-t-il par rapport à *TLS* sans *SNI* ?

4- Sécurité (7 points)

A. Attaque par canaux auxiliaires

Expliquez ce qu'est une attaque par canaux auxiliaires (*Side-channel attack*).

Présentez une méthode d'attaque qui utilise un canal auxiliaire.

Présentez une méthode d'attaque qui n'utilise pas de canal auxiliaire.

B. Spectre/Meltdown

Expliquez rapidement le principe des attaques *Spectre* et *Meltdown*.

Quel type de matériel ou de logiciel est concerné par cette faille ?

Quels correctifs permettent de s'assurer d'une protection contre ces attaques ?

C. Blockchain

Qu'est-ce qu'une *blockchain* ?