

Corrigé PSE 2021 : systèmes, réseau et sécurité

Proposition de corrigé — non officielle. Examen professionnel 2021, épreuve écrite n° 1. Les quatre parties sont traitées ; les conventions de temps de réponse et de commutation sont précisées.

[Sujet officiel](#) · [Annales de ce concours ou examen](#)

1A. Isolation des processus et tubes nommés

Le système donne à chaque processus un espace d'adressage virtuel, protège les pages mémoire et contrôle les accès aux ressources. Droits et modes utilisateur/noyau évitent qu'un processus accède librement à celui d'un autre. Sous Linux, **espaces de noms et groupes de contrôle** peuvent en outre isoler la visibilité de ressources et limiter leur consommation ; une machine virtuelle constitue un autre niveau d'isolation. Isolation mémoire, cloisonnement et quotas ne sont pas exactement la même fonction.

Un **tube nommé**, ou FIFO sous UNIX, possède un nom dans le système de fichiers. Des processus l'ouvrent pour écrire et lire un flux d'octets, dans l'ordre ; ils n'ont pas besoin d'être issus du même parent. Permissions et synchronisation bloquante facilitent une communication locale simple. En contrepartie, il faut gérer blocage, fermeture, lectures partielles et absence de frontières de messages. Pour un échange bidirectionnel, on peut employer deux FIFO ou préférer un socket. Une FIFO UNIX n'est pas, à elle seule, une connexion réseau ; les tubes nommés Windows disposent d'autres possibilités.

1B. Ordonnancement

FCFS sert les processus dans l'ordre d'arrivée, sans préemption : simple, mais une tâche longue peut retenir toutes les petites. **SJF** choisit le travail le plus court ; il réduit l'attente moyenne dans le modèle où les durées sont connues, mais demande leur estimation et peut retarder les tâches longues. **RR**, tourniquet, attribue un quantum à chacun, puis replace une tâche inachevée en queue : il favorise une première réponse rapide, au prix de commutations.

Un algorithme **préemptif** peut retirer le CPU à une tâche avant qu'elle termine ou se bloque. Le SJF utilisé ici est non préemptif ; sa variante préemptive est le plus court temps restant. RR est préemptif.

1. Gantt sans coût de commutation

Les cinq tâches arrivent à $t = 0$, dans l'ordre donné. Les durées sont $P_1 = 7$, $P_2 = 1$, $P_3 = 2$, $P_4 = 1$ et $P_5 = 5$ ms. En cas d'égalité SJF, on conserve l'ordre d'arrivée.

```
FCFS : 0--P1--7-P2-8--P3--10-P4-11---P5---16
SJF   : 0-P2-1-P4-2--P3--4---P5---9----P1----16
RR 1  : [0,1] P1 ; [1,2] P2 ; [2,3] P3 ; [3,4] P4
        [4,5] P5 ; [5,6] P1 ; [6,7] P3 ; [7,8] P5
        [8,9] P1 ; [9,10] P5 ; [10,11] P1 ; [11,12] P5
```

[12,13] P1 ; [13,14] P5 ; [14,15] P1 ; [15,16] P1

L'expression « temps de réponse » est ambiguë. En ordonnancement interactif, c'est le **délai jusqu'à la première exécution** ; certains exercices l'emploient pour le **temps de séjour**, jusqu'à la fin. Voici les deux mesures, avec l'attente totale, pour éviter de les confondre.

Algorithme	Premiers départs P_1 à P_5	Fins P_1 à P_5	Première réponse moyenne	Séjour moyen	Attente moyenne
FCFS	0 ; 7 ; 8 ; 10 ; 11	7 ; 8 ; 10 ; 11 ; 16	7,2 ms	10,4 ms	7,2 ms
SJF	9 ; 0 ; 2 ; 1 ; 4	16 ; 1 ; 4 ; 2 ; 9	3,2 ms	6,4 ms	3,2 ms
RR, q = 1	0 ; 1 ; 2 ; 3 ; 4	16 ; 2 ; 7 ; 4 ; 14	2 ms	8,6 ms	5,4 ms

Le séjour est la date de fin puisque toutes les arrivées valent zéro. L'attente totale vaut séjour moins durée CPU ; elle n'est égale à la première réponse que dans les deux ordonnancements non préemptifs considérés.

2. Commutation de 0,5 ms et quantum

On compte 0,5 ms **lors d'un changement de processus**, pas avant le premier départ ni lorsque P_1 continue seul à la fin.

SJF : P2 [0,1] ; P4 [1.5,2.5] ; P3 [3,5]
P5 [5.5,10.5] ; P1 [11,18]
RR : P1 [0,1] ; P2 [1.5,2.5] ; P3 [3,4] ; P4 [4.5,5.5]
P5 [6,7] ; P1 [7.5,8.5] ; P3 [9,10] ; P5 [10.5,11.5]
P1 [12,13] ; P5 [13.5,14.5] ; P1 [15,16]
P5 [16.5,17.5] ; P1 [18,19] ; P5 [19.5,20.5]
P1 [21,22] puis [22,23]

Algorithme	Première réponse moyenne	Séjour moyen	Attente moyenne
SJF	4,2 ms	7,4 ms	4,2 ms
RR, q = 1	3 ms	12,3 ms	9,1 ms

Avec un quantum de 1 ms, une commutation de 0,5 ms est coûteuse : RR garde une première réponse rapide mais dégrade le séjour. **Il n'existe pas un quantum optimal sans critère de performance.** Dans ce lot et pour des quanta entiers, q = 2 ms donne un séjour moyen de 11,3 ms, le plus faible parmi q = 1 à 7 ; q = 1 garde la meilleure première réponse. À q ≥ 7, RR devient ici FCFS, avec séjour moyen 11,4 ms. Augmenter le quantum réduit les commutations mais diminue la réactivité ; ces résultats ne constituent pas une règle universelle.

2. Termes et acronymes

Terme	Définition
ACPI	Advanced Configuration and Power Interface : interface de configuration matérielle et de gestion de l'énergie.
AMQP	Advanced Message Queuing Protocol : protocole de messagerie pour échanges via des intermédiaires et files, selon les mécanismes prévus.
BaaS	Backend as a Service : services de backend accessibles à une application. L'abréviation peut aussi désigner Backup as a Service ou Blockchain as a Service ; le contexte doit être précisé.
DKIM	DomainKeys Identified Mail : signature de parties d'un courriel, vérifiée avec une clé publiée dans le DNS. Elle authentifie un domaine signataire, pas la véracité du message.
Deep Scrolling	Terme d'interface, non acronyme normalisé : défilement long ou continu, éventuellement avec chargement progressif, plutôt qu'une navigation par pages.
i18n	Internationalisation : 18 lettres entre i et n. Préparer un logiciel aux langues, formats, textes et conventions locales.
SIEM	Security Information and Event Management : collecte, corrélation et analyse d'événements de sécurité.
Infonébulisation	Fog computing : traitement et stockage distribués sur des nœuds proches des équipements, entre objets connectés et services cloud ; réduction de la latence et des transferts.

3A. HTTP/1.1 et HTTP/2

Le **pipelining HTTP/1.1** permet d'envoyer plusieurs requêtes sur une connexion sans attendre chaque réponse. Les réponses restent ordonnées, ce qui peut bloquer celles placées derrière une réponse lente.

Le **multiplexage HTTP/2** entrelace les trames de plusieurs flux sur une même connexion. Chaque flux est identifié, ce qui évite l'obligation d'achever toutes les réponses dans l'ordre des requêtes.

Compression des en-têtes et contrôle des flux contribuent aussi au fonctionnement. Le pipelining n'est donc pas une invention propre à HTTP/2. En 2021, HTTP/2 sur TCP reste exposé au blocage dû à la perte d'un segment TCP au niveau du transport.

3B. Fragmentation IPv4

La fragmentation divise un datagramme qui dépasse le **MTU**, taille maximale du paquet IP transportable sur un lien. Si le bit DF interdit cette opération, le routeur ne fragmente pas et signale le problème selon le protocole. En IPv4, la **destination finale** réassemble : un routeur intermédiaire n'a pas nécessairement tous les fragments, notamment si les chemins diffèrent.

Le MTU Ethernet standard est généralement **1 500 octets** pour le paquet IP, hors en-têtes Ethernet ; il peut être configuré autrement. `tracert` peut estimer le MTU du chemin ; `ip link` décrit celui d'une interface locale, sans prouver le MTU de tout le trajet. Des sondes avec DF donnent une autre méthode si les réponses nécessaires ne sont pas bloquées.

Réseau A : MTU 1 024

Le datagramme comprend 20 octets d'en-tête et **2 684 octets de données**. Le plus grand fragment non final transporte un multiple de huit octets : $\lfloor (1024 - 20)/8 \rfloor \times 8 = 1\ 000$. Le décalage est mesuré en unités de huit octets depuis les données du datagramme initial.

Fragment A	Données	Total Length	Fragment Offset	MF
A1	1 000	1 020	0	1
A2	1 000	1 020	125	1
A3	684	704	250	0

Réseau B : MTU 512

Les routeurs refragmentent chacun des fragments reçus : charge maximale non finale **488 octets**. Ils ne réassemblent pas d'abord les 2 684 octets pour repartir de zéro.

Fragment B	Données	Total Length	Fragment Offset	MF
B1, issu de A1	488	508	0	1
B2, issu de A1	488	508	61	1
B3, issu de A1	24	44	122	1
B4, issu de A2	488	508	125	1
B5, issu de A2	488	508	186	1
B6, issu de A2	24	44	247	1
B7, issu de A3	488	508	250	1
B8, issu de A3	196	216	311	0

Seul B8 termine le datagramme initial : les derniers sous-fragments de A1 et A2 gardent MF = 1. Tous conservent l'identification commune du datagramme, avec les autres adaptations d'en-tête requises.

4A. Concepts de sécurité

IDS : système de détection d'intrusion, sur un hôte — HIDS — ou sur le réseau — NIDS. Il peut reconnaître des signatures, des anomalies ou des comportements selon ses modèles. Il alerte et produit des traces ; un IPS peut en plus intervenir pour bloquer. Faux positifs, chiffrement et visibilité limitent la détection.

PKI : infrastructure de gestion de clés publiques et de certificats. Une autorité de certification signe le lien entre identité et clé publique ; le destinataire vérifie chaîne de confiance, validité, usages et révocation selon le mécanisme disponible. La clé privée reste protégée. Un certificat valide ne prouve pas que tout le contenu fourni est honnête.

Signature aveugle : le demandeur masque un message, le fait signer puis retire le masque pour obtenir une signature vérifiable du message initial. Dans un protocole approprié, le signataire ne peut relier simplement l'émission à l'usage. Un jeton de paiement électronique ou de vote peut s'appuyer sur ce principe ; empêcher double dépense ou double vote demande des mécanismes supplémentaires.

4B. Attaques et réponses

Trois attaques DNS

Empoisonnement de cache : introduire une fausse réponse pour rediriger. Validation DNSSEC, configuration correcte du résolveur et protections du protocole réduisent ce risque ; DNSSEC ne chiffre pas les requêtes.

Déni de service par réflexion/amplification : des réponses DNS sont envoyées vers une victime avec adresse source usurpée. Éviter les résolveurs récurifs ouverts, filtrer les adresses usurpées et limiter les réponses contribue à la défense, avec une capacité de mitigation réseau.

Détournement du domaine ou de sa configuration : compromettre un compte de registraire ou d'administration modifie les serveurs ou enregistrements. Authentification forte, moindre privilège, verrouillage adapté et suivi des changements protègent cette chaîne. Le seul cache local n'est alors pas la cause.

Chaîne d'approvisionnement

L'attaque compromet un fournisseur, une dépendance, un outil de construction ou une mise à jour pour atteindre les utilisateurs. Inventaire des composants, contrôle des fournisseurs, signatures et provenance des paquets, environnement de construction protégé et tests limitent l'exposition. Une signature réalisée avec une clé compromise n'est pas une garantie suffisante ; limiter les privilèges et pouvoir retirer une version restent nécessaires.

APT

Une **Advanced Persistent Threat** vise une présence durable et discrète, généralement au service d'un objectif ciblé. Elle peut combiner compromission initiale, persistance, déplacement et collecte. Détection comportementale, segmentation, correctifs, contrôle des identités et réponse coordonnée doivent couvrir la durée ; il ne s'agit pas simplement d'un virus plus complexe.

Attaque des 51 %

Dans une chaîne à preuve de travail, une majorité de puissance de calcul peut favoriser une chaîne concurrente, censurer ou réorganiser des transactions et tenter une double dépense de ses propres fonds. Cela ne donne pas les clés privées des autres utilisateurs ni le pouvoir de produire n'importe quelle transaction valide.

La défense repose notamment sur une puissance honnête suffisante et distribuée, l'absence de concentration excessive et des confirmations adaptées au risque. Des mécanismes de finalité ou points de contrôle peuvent changer le modèle, avec d'autres hypothèses de confiance. Renforcer uniquement la fonction de hachage ne résout pas une majorité de calcul hostile ; aucune mesure ne garantit universellement l'absence de cette attaque dans tous les protocoles.

Références

[RFC 791](#), [IPv4](#), [RFC 7540](#), [HTTP/2](#), [NIST SP 800-94](#), [détection d'intrusion](#), [RFC 5280](#), [certificats](#), [RFC 4033](#), [DNSSEC](#), [article fondateur de Bitcoin](#). Les calculs d'ordonnancement utilisent les cinq tâches de l'énoncé.