Découverte de Tor : fiche « nœud intermédiaire »

1 Votre rôle

Vous êtes un **nœud intermédiaire**. Vous représentez un serveur participant au projet Tor et destiné à participer à un circuit Tor. Votre rôle est de passer à un **nœud de sortie** des messages provenant d'un **nœud d'entrée**. Ces messages sont rédigés par un **émetteur** et adressés à un **destinataire**, tous deux situés hors du circuit Tor. De même, vous serez amené à transmettre les réponses du destinataire à l'émetteur par le même chemin.

2 Organisation

Les participants sont répartis en cinq groupes :
- Les émetteurs ;
- Les nœuds d'entrée ;
- Les nœuds intermédiaires (dont vous faites partie) ;
- Les nœuds de sortie ;
- Les destinataires.

Vous disposez du matériel suivant :
- Des enveloppes de taille moyenne (optionnel) ;
- Un crayon, une gomme ;
- La présente fiche.

3 Transmettre un message provenant d'un nœud d'entrée

Un enveloppe représente le chiffrement utilisé pour protéger un message, et seules les personnes possédant la clé de déchiffrement peuvent l'ouvrir. On suppose que l'émetteur possède une copie de votre clé.

Un nœud d'entrée peut être amené à vous transmettre un message, sous la forme d'une enveloppe de taille moyenne.

1. Vérifiez que vous êtes bien identifié comme pouvant ouvrir cette enveloppe (il doit y avoir indiqué « chiffré avec la clé de : … » sur l'enveloppe) ;
2. Notez le numéro de circuit indiqué sur l'enveloppe et regardez dans le tableau ci-dessous si le couple (nœud d'entrée - numéro de circuit amont) est déjà présent.
   Si c'est le cas :
   (a) Ouvrez l'enveloppe et sortez-en une enveloppe de petite taille (cela simule le déchiffrement de la couche intermédiaire du chiffrement en oignon) ;
   (b) Prenez connaissance de l'identité du nœud Tor capable de déchiffrer l'enveloppe de petite taille et vérifiez qu'il correspond bien à la ligne du tableau que vous avez identifiée ;
   (c) Inscrivez sur l'enveloppe de petite taille « numéro de circuit : » suivi du numéro de circuit aval correspondant dans le tableau ;
   (d) Transmettez l'enveloppe de petite taille au nœud de sortie désigné ;
   (e) Effacez les inscriptions sur l'enveloppe de taille moyenne et conservez-la pour une utilisation ultérieure.
   Si ce n'est pas le cas :
   (a) Ajoutez une entrée dans le tableau en renseignant les deux premières colonnes avec ces informations ;
   (b) Ouvrez l'enveloppe et sortez-en une enveloppe de petite taille (cela simule le déchiffrement de la couche intermédiaire du chiffrement en oignon) ;

(c) Prenez connaissance de l'identité du nœud Tor capable de déchiffrer l'enveloppe de petite taille ;

(d) Attribuez un numéro de circuit unique et renseignez les deux dernières colonnes du tableau ;

(e) Inscrivez sur l'enveloppe de petite taille « numéro de circuit : » suivi du numéro de circuit aval que vous venez de choisir ;

(f) Transmettez l'enveloppe de petite taille au nœud de sortie désigné ;

(g) Effacez les inscriptions sur l'enveloppe de taille moyenne et conservez-la pour une utilisation ultérieure.

Nœud d'entrée	Numéro de circuit amont	Nœud de sortie	Numéro de circuit aval

4 Transmettre un message provenant d'un nœud de sortie

Un nœud de sortie peut vous transmettre une enveloppe de petite taille, qui correspond à une réponse en train d'être acheminée depuis un destinataire vers un émetteur. Comme vous pouvez participer à plusieurs circuits simultanément, le tableau que vous avez construit vous aidera à identifier l'émetteur concerné.

1. Vérifiez que le nœud de sortie qui vous transmet l'enveloppe et le numéro de circuit qui est inscrit dessus correspond bien au couple (nœud de sortie, numéro de circuit aval) de l'une des lignes de votre tableau ;
2. Identifiez le nœud d'entrée et le numéro de circuit amont correspondants grâce au tableau ;
3. Placez l'enveloppe de petite taille dans une enveloppe de taille moyenne en inscrivant dessus « chiffré avec la clé de : » suivi de votre identité ;
4. Inscrivez sur l'enveloppe de taille moyenne « numéro de circuit : » suivi du numéro de circuit amont que vous venez d'identifier ;
5. Transmettez l'enveloppe au nœud d'entrée que vous avez identifié.

5 Conclusions

- En tant que nœud intermédiaire, pouvez-vous identifier l'émetteur d'un échange de messages ?
- En tant que nœud intermédiaire, pouvez-vous identifier le destinataire d'un échange de messages ?
- Pouvez-vous identifier le nœud d'entrée du circuit ?
- Pouvez-vous identifier le nœud de sortie du circuit ?
- Que devrions-nous changer dans le protocole pour modifier la réponse aux deux questions précédentes ?
- En tant que nœud intermédiaire, connaissez-vous le contenu d'un échange de messages ?
- Qu'est-ce qui changera pour vous si l'émetteur décide d'utiliser, en plus de Tor, un chiffrement dit « de bout en bout » entre lui et le destinataire (comme dans le cas d'une communication HTTPS) ?
- Quel est l'intérêt des numéros de circuits ? Pourrait-on s'en passer ? Pourquoi ?