Découverte de Tor : fiche « nœud de sortie »

1 Votre rôle

Vous êtes un **nœud de sortie**. Vous représentez un serveur participant au projet Tor et destiné à participer à un circuit Tor. Votre rôle est de faire sortir un message (passé par un **nœud intermédiaire**) du circuit Tor et de le remettre à son **destinataire**. Ce message provient initialement d'un **émetteur**, qui l'a fait transiter par un **nœud d'entrée**. 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 ;
- Les nœuds de sortie (dont vous faites partie) ;
- Les destinataires.

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

3 Transmettre un message provenant d'un nœud intermédiaire

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 intermédiaire peut être amené à vous transmettre un message, sous la forme d'une enveloppe de petite taille.

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 intermédiaire - numéro de circuit) est déjà présent.
   Si c'est le cas :
   (a) Ouvrez l'enveloppe et sortez-en le message (cela simule le déchiffrement de la couche interne du chiffrement en oignon) ;
   (b) Prenez connaissance de l'identité du destinataire et vérifiez qu'il correspond bien à la ligne du tableau que vous avez identifiée ;
   (c) Vérifiez que l'identifiant du flux TCP indiqué sur le message correspond bien à cette entrée du tableau, sinon ajoutez-le (une même ligne peut contenir plusieurs identifiants TCP) ;
   (d) Renseignez le champ « émetteur : » du message avec votre propre identité ;
   (e) Transmettez le message au destinataire ;
   (f) Effacez les inscriptions sur l'enveloppe de petite taille 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 le message (cela simule le déchiffrement de la couche interne du chiffrement en oignon) ;

(c) Prenez connaissance de l'identité du destinataire et de l'identifiant de flux TCP du message (l'identifiant TCP est une notion indépendante de Tor : elle permet, dans un échange TCP, de faire correspondre les messages envoyés et leurs réponses sans risque de confusion) ;

(d) Renseignez les deux dernières colonnes du tableau avec ces informations ;

(e) Renseignez le champ « émetteur : » du message avec votre propre identité ;

(f) Transmettez le message au destinataire ;

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

Nœud intermédiaire	Numéro de circuit	Destinataire	Identifiant TCP

4 Transmettre un message provenant d'un destinataire

Un destinataire peut vous faire parvenir une réponse au message que vous lui avez transmis. Comme le destinataire et vous pouvez participer à plusieurs flux d'informations simultanément, le tableau que vous avez construit vous aidera à identifier l'émetteur concerné.

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

5 Conclusions

– En tant que nœud de sortie, pouvez-vous identifier l'émetteur d'un échange de messages ?
– En tant que nœud de sortie, pouvez-vous identifier le destinataire d'un échange de messages ?
– Pouvez-vous identifier le nœud d'entrée du circuit ?
– Pouvez-vous identifier le nœud intermédiaire du circuit ?
– 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 et des identifiants TCP ? Pourrait-on s'en passer ? Pourquoi ?