Découverte de Tor : fiche « émetteur »

1 Votre rôle

Vous êtes un **émetteur**. Vous représentez l'ordinateur d'un utilisateur cherchant à communiquer avec un serveur web (le **destinataire**) en passant par le réseau Tor. Vous devrez pour cela faire transiter vos messages par un circuit Tor comprenant un **nœud d'entrée**, un **nœud intermédiaire** et un **nœud de sortie**. Le destinataire devra pouvoir vous faire parvenir une réponse par le même circuit.

2 Organisation

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

Vous disposez du matériel suivant :
- Des enveloppes de grande taille ;
- Des enveloppes de taille moyenne ;
- Des enveloppes de petite taille ;
- Des feuilles de papier entrant dans les petites enveloppes ;
- Un crayon, une gomme ;
- La présente fiche.

3 Envoyer un message

3.1 Construire le circuit

1. Choisir un nœud d'entrée, un nœud intermédiaire, un nœud de sortie et un destinataire ;
2. On suppose que vous partagez un secret (une clé de chiffrement) avec chacun des nœuds Tor.

3.2 Préparer le message pour le destinataire

1. Sur une feuille de papier, inscrivez « Émetteur : » en laissant le champ vide, puis « Destinataire : » en indiquant le nom du destinataire que vous avez choisi ;
2. Inscrivez « Identifiant du flux TCP : « suivi d'un nombre (assez grand) choisi au hasard (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) ;
3. Inscrivez un message pour le destinataire, par exemple une question à laquelle il devra répondre. Ne donnez pas d'indication quant à votre identité.

3.3 Préparer le message pour le nœud de sortie

Le message que vous avez écrit sera au final délivré par le nœud de sortie de votre circuit. Le message devra lui arriver chiffré, et c'est lui qui le déchiffrera et le transmettra. En conséquence :

1. Placez votre message dans une petite enveloppe ;
2. Inscrivez sur l'enveloppe « chiffré avec la clé de : » suivi du nom de votre nœud de sortie que vous avez choisi (ceci simule le chiffrement avec la clé que vous partagez avec le nœud de sortie).

3.4 Préparer le message pour le nœud intermédiaire

1. Placez la petite enveloppe dans une enveloppe de taille moyenne ;
2. Inscrivez sur l'enveloppe « chiffré avec la clé de : » suivi du nom de votre nœud intermédiaire.

3.5 Préparer le message pour le nœud d'entrée

1. Placez l'enveloppe de taille moyenne dans une grande enveloppe ;
2. Inscrivez sur l'enveloppe « chiffré avec la clé de : » suivi du nom de votre nœud d'entrée.

3.6 Envoyer le message

Donnez la grande enveloppe à votre nœud d'entrée.

4 Recevoir une réponse

Normalement, le nœud d'entrée devrait vous remettre une grande enveloppe avec l'inscription « chiffré avec la clé de : » suivi de votre nom.

1. Ouvrez la grande enveloppe (si elle est chiffrée avec une clé que vous connaissez) ;
2. Ouvrez l'enveloppe moyenne (si elle est chiffrée avec une clé que vous connaissez) ;
3. Ouvrez la petite enveloppe (si elle est chiffrée avec une clé que vous connaissez) ;
4. Prenez connaissance de la réponse à votre message. Vérifiez son émetteur et l'identifiant de flux TCP.

5 Conclusions

- Parmi les divers acteurs avec lesquels vous avez communiqué, lesquels connaissent votre identité ?
- Parmi les divers acteurs avec lesquels vous avez communiqué, lesquels connaissent l'identité du destinataire ?
- Parmi les divers acteurs avec lesquels vous avez communiqué, lesquels connaissent le contenu du message et de sa réponse ?
- Que faudrait-il changer aux manipulations que vous avez effectuées si vous souhaitiez mettre en place un chiffrement dit « de bout en bout » entre votre destinataire et vous (comme dans le cas d'une communication HTTPS) ?