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) ?

Découverte de Tor : fiche « nœud d'entrée »

1 Votre rôle

Vous êtes un **nœud d'entrée**. Vous représentez un serveur participant au projet Tor, destiné à être en contact direct avec les utilisateurs (**émetteurs**) en tant que premier élément du circuit qu'ils auront choisi pour joindre le **destinataire**. Votre rôle est de faire transiter les messages de l'émetteur au destinataire via un **nœud intermédiaire** et un **nœud de sortie**. 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 (dont vous faites partie) ;
— Les nœuds intermédiaires ;
— Les nœuds de sortie ;
— Les destinataires.

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

3 Transmettre un message de l'émetteur

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 émetteur peut choisir de vous transmettre un message sous la forme d'une enveloppe de grande 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. Ouvrez l'enveloppe et sortez-en une enveloppe de taille moyenne (cela simule le déchiffrement de la couche extérieure du chiffrement en oignon) ;
3. Prenez connaissance de l'identité du nœud Tor capable de déchiffrer l'enveloppe de taille moyenne ;
4. Attribuez à cette association entre l'émetteur et le nœud désigné un **numéro de circuit** que vous conserverez dans le tableau suivant (à moins que cette association ne vous soit déjà connue) :

Émetteur	Nœud intermédiaire	Numéro de circuit attribué

5. Inscrivez sur l'enveloppe de taille moyenne « numéro de circuit : » suivi de ce numéro ;
6. Transmettez l'enveloppe de taille moyenne au nœud intermédiaire désigné ;
7. Effacez les inscriptions sur l'enveloppe de grande taille et conservez-la pour une utilisation ultérieure.

4 Transmettre un message provenant d'un autre nœud Tor

Un nœud intermédiaire peut vous transmettre une enveloppe de taille moyenne, 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 qui vous transmet l'enveloppe et le numéro de circuit qui est inscrit dessus correspond bien à l'une des lignes de votre tableau ;
2. Identifiez l'émetteur grâce au tableau ;
3. Placez l'enveloppe de taille moyenne dans une enveloppe de grande taille en inscrivant dessus « chiffré avec la clé de : » suivi de votre nom ;
4. Transmettez l'enveloppe à l'émetteur.

5 Conclusions

— En tant que nœud d'entrée, pouvez-vous identifier l'émetteur d'un échange de messages ?
— En tant que nœud d'entrée, pouvez-vous identifier le récepteur d'un échange de messages ?
— Pouvez-vous identifier le nœud intermédiaire du circuit ?
— Pouvez-vous identifier le nœud de sortie du circuit ?
— En tant que nœud d'entrée, 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 ?

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 ?

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 ?

Découverte de Tor : fiche « destinataire »

1 Votre rôle

Vous êtes le **destinataire** d'un message, composé par un **émetteur** qui souhaite le faire transiter par un circuit Tor. Il le transmettra à un **nœud d'entrée**, puis à un **nœud intermédiaire**, puis à un **nœud de sortie**, qui vous l'enverra directement. De même, vous serez amené à envoyer vos réponses 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 ;
— Les destinataires (dont vous faites partie).

Vous disposez du matériel suivant :

— Des feuilles de papier entrant dans les petites enveloppes ;
— Un crayon, une gomme ;
— La présente fiche.

3 Transmettre un message provenant d'un nœud de sortie

Un enveloppe représente le chiffrement utilisé pour protéger un message, et seules les personnes possédant la clé de chiffrement peuvent l'ouvrir. Dans cette version de l'exercice, vous n'aurez pas à manipuler d'enveloppe.

Un nœud de sortie peut être amené à vous transmettre un message.

1. Vérifiez que vous êtes bien identifié comme le destinataire de ce message, et prenez connaissance de son émetteur ;
2. Notez l'identifiant TCP indiqué sur l'enveloppe ;
3. Sur une nouvelle feuille, indiquez « émetteur : » suivi de votre identité, « destinataire : » suivi de l'identité de l'émetteur du message que vous venez de recevoir et « identifiant TCP : » suivi du numéro présent sur le message que vous venez de recevoir ;
4. Écrivez une réponse au message ;
5. Transmettez votre message au destinataire que vous avez identifié, à savoir le nœud de sortie qui vous l'a transmis.

4 Conclusions

— En tant que destinataire, pouvez-vous identifier l'émetteur d'un échange de messages ?
— En tant que destinataire, connaissez-vous le contenu du message ?
— Pouvez-vous identifier le nœud d'entrée du circuit Tor ?
— Pouvez-vous identifier le nœud intermédiaire du circuit Tor ?
— Pouvez-vous identifier le nœud de sortie du circuit Tor ?
— Qu'est-ce qui pourrait vous permettre de savoir que la personne qui vous a transmis le message n'est pas celle qui l'a rédigée ?
— Qu'est-ce qui pourrait vous permettre de savoir que le message est passé par un circuit Tor ?
— 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 vous (comme dans le cas d'une communication HTTPS) ?
— Quel est l'intérêt de l'identifiant TCP ? Pourrait-on s'en passer ? Pourquoi ?