Analyse d'applications réseaux

1 Contexte du projet

En tant qu'ingénieur·e réseau, il est important de pouvoir comprendre le fonctionnement des protocoles qui constituent l'Internet et également le comportement de ses applications. C'est en combinant ces deux savoirs qu'un·e ingénieur·e réseau peut à la fois améliorer les protocoles de l'Internet et concevoir des applications réseaux efficaces.

Dans ce projet, vous analyserez une application réseau intégrant des fonctionnalités de stockage et partage de fichiers. Ce type d'application est très commun et comporte beaucoup de comportements différents, chacun alliant des exigences particulières se traduisant en des utilisations et combinaisons de protocoles différentes.

Par groupe de deux, vous étudierez comment les différentes fonctionnalités de l'application considérée sont implémentées en observant le trafic réseau produit par celle-ci. Vous produirez un rapport de 4 pages résumant vos observations appuyées par des captures de paquets. Vous trouverez dans ce document les lignes directrices nécessaires pour mener à bien cette étude, les délivrables attendus et l'échéance définie.

2 Méthode d'analyse

Commencez par découvrir toutes les fonctionnalités de l'application étudiée. Parcourez-la et énumérez ce qu'elle permet de faire. Sur base des fonctionnalités découvertes, créez un ou plusieurs scénarios de tests permettant de les parcourir de façon systématique. Cela vous permettra de répéter les mêmes actions dans l'application dans des conditions réseaux différentes (par ex. connecté en Wi-Fi, Ethernet ou partage 4G).

À l'aide de `tcpdump` ou Wireshark, lancez une capture de paquets. Pour observer un maximum de comportements, choisissez l'interface de capture `any` qui reprendra l'entièreté des paquets échangés, peu importe leur provenance (Ethernet, Wi-Fi, etc). Vérifiez à bien identifier les paquets qui proviennent de votre application. Afin de faciliter votre analyse du trafic, il est important de stopper *toutes* les autres applications susceptibles d'utiliser Internet pendant le test. Une fois la capture lancée, démarrez l'application et exécutez votre scénario de test et stoppez la capture une fois terminé [1]. Il peut vous être utile de capturer votre écran lorsque vous exécutez votre scénario. Cela vous permettra par après de mieux comprendre le lien entre votre utilisation de l'application et l'activité observée sur le réseau. Avec certaines applications, il est possible de stocker les secrets échangés en créant une variable d'environement **SSLKEYLOGFILE** avec un chemin vers un fichier. Il est alors possible de déchiffer le contenu des paquets dans Wireshark en indiquant ce chemin dans *Edit->Preferences->Protocols->TLS->(Pre)-Master-Secret log filename.*

2.1 Analyse des traces

Les questions reprisent dans cette sous-section sont un point de départ de votre réflexion. Elles vous permettent de vous donner des pistes d'analyses des différents protocoles. Il est attendu de vous que vous interprétiez et expliquiez l'utilité des fonctionnalités des protocoles utilisés lorsque vous le pouvez. Il est important d'être factuel et de vérifier vos affirmations en citant des faits ou des références. Il peut vous être utile de produire des graphes ou tableaux pour soutenir vos explications [2]. Donnez toujours le contexte dans lequel vous avez observé ces faits.

1. Il peut être intéressant de garder quelques secondes d'inactivité à la fin du scénario de test pour observer des comportements retardés.
2. Soyez attentif à la taille de ceux-ci, minimiser la en gardant une certaine lisibilité.

Lors de votre analyse des traces, il peut vous être utile de développer des scripts qui extrairont et calculeront des statistiques de votre choix sur base des fichiers de capture de paquets. Vous pouvez utiliser par exemple la librairie Python `pyshark` pour cela.

2.1.1 DNS

- Combien de noms de domaines sont résolus et quand ?
- Quels sont les serveurs autoritatifs pour ces noms de domaines ? Sont-ils gérés par des entreprises différentes ?
- À quelles entreprises appartiennent les noms de domaines résolus ? Il y en a-t-il d'autres que celle qui détient l'application ?
- Quels sont les types de requête DNS effectuées ?
- Lorsqu'une requête DNS souhaite obtenir une adresse IP, quelle est sa famille ? Il y a-t-il une version IP préférée par l'application ?
- Les requêtes contiennent elles des records additionnels ? Le cas échéant, à quoi servent-ils ?
- Observez-vous des comportements DNS inattendus ?

2.1.2 Couche réseau

- Lorsque IPv4 est utilisé, l'application utilise-t-elle des techniques pour traverser les NAT [3].
- Quels sont les adresses vers lesquels des paquets sont envoyés ? Retrouvez à quels noms de domaine elles correspondent, observez-vous une tendance particulière dans la famille d'adresse ? Pouvez-vous l'expliquer ?

2.1.3 Couche transport

- Quels sont les protocoles de transports utilisés pour chaque fonctionnalité ?
- Il y a-t-il plusieurs connexions vers un même nom de domaine ? Si oui, pouvez-vous l'expliquer ?
- Si vous observez du trafic QUIC, quels sont les versions utilisées ? Pouvez-vous identifier des extensions négociées dans le handshake ?
- Lorsque vous observez du trafic UDP, identifiez-vous d'autres protocoles que QUIC et DNS ? Expliquez comment ils sont utilisés par l'application.

2.1.4 Chiffrement et sécurité

- L'utilisation du DNS est-elle sécurisée ? Comment ?
- Quelles versions de TLS sont utilisées ? Précisez les protocoles de transport sécurisés par ces versions.
- Quel est la durée de vie des certificats utilisés ? Par qui sont-ils certifiés ?
- Lorsque vous pouvez observer l'établissement du chiffrement, quels sont les algorithmes de chiffrement utilisés ?
- Si vous observez du trafic UDP, semble-t-il chiffré ? Comment est-il sécurisé ?

2.1.5 Application

- Quels comportements observer-vous lors du transfert de nouveaux fichiers comparé à la modification de fichiers existant ? Quel impact a la modification par plusieurs utilisateurs par rapport à un seul ?
- Quel est le volume de données échangées par l'application pour chacune de ces fonctionnalités ? Utilisez une base appropriée permettant la comparaison (par ex. par minute).

3. Les NAT étant propres à IPv4, le cours ne les aborde pas. Une bonne ressource est `https://www.cisco.com/c/dam/en_us/about/ac123/ac147/archived_issues/ipj_7-3/ipj_7-3.pdf`

— Il y a-t-il des serveurs relais utilisés pour interagir avec un utilisateur ou les applications communiquent-elles directement ? Observez-vous autre chose lorsque deux utilisateurs sont sur le même réseau Wi-Fi [4] ?
— Est-ce qu'interagir avec un utilisateur se trouvant dans le même réseau Wi-Fi ou Ethernet a un impact sur la façon dont le trafic applicatif est transporté ? Il y a-t-il des serveurs relais ?

3 Délivrables et échéance

Votre rapport de 4 pages au format double colonnes est attendu pour le 29 mars 2024 à 12 h. Il utilisera le modèle de rapport disponible sur Moodle. Le rapport contiendra un lien vers un dépôt `git` contenant vos captures ainsi que les éventuels scripts utilisés au cours du projet. La soumission du rapport se fera sur HotCRP et sera annoncée sur Moodle. Restez succinct lors de la présentation de l'application. Ce sont bien vos mesures, analyses et interprétations qui seront évaluées. Il n'est pas attendu de vous d'étudier toutes les fonctionnalités de l'application réseau. Il vous faut sélectionner les plus pertinentes et fournir un maximum d'analyses et d'interprétations de vos observations dans le rapport.

4. Le réseau `eduroam` isole les utilisateurs, observez plutôt ce qui se passe dans un réseau domestique.