Analyse d'applications réseaux

1st Louis Bauchau
Université Catholique de Louvain
Sciences Informatiques
Belgique
louis.bauchau@student.uclouvain.be

2nd Maxim Thomas
Université Catholique de Louvain
Sciences Informatiques
Belgique
maxim.thomas@student.uclouvain.be

I. Introduction

Dans le cadre du cours de réseau LINFO 1341 à l'Université Catholique de Louvain, nous allons analyser une application intégrant des fonctionnalités de conversation et de visio-conférence. L'application que notre groupe va analyser est Zoom.

II. Méthode d'analyse

Afin d'analyser les fonctionnalités disponibles dans Zoom, nous avons utilisé Wireshark. Cet outil nous a permis de créer des traces réseaux lors de la réalisation de nos scénarios de tests.(cf. [1])

Les différentes fonctionnalités de Zoom reprises dans nos scénarios de tests sont les suivantes:

- La création d'une réunion.
- Rejoindre une réunion.
- L'envoi et la réception de messages textuels.
- L'envoi et la réception de messages audio.
- L'envoi et le réception de flux vidéo.
- Le partage d'écran.
- La création d'un tableau blanc.

Enfin Pour améliorer notre analyse de trace, nous avons utilisé un filtre global nous permettant d'isoler le trafic réseau. (cf. [2])

Nous n'avons pas utilisé GIT pour le projet, nous avons préférés utiliser un OneDrive partagé avec les différentes traces et notes manuscrites.

Cependant nous avons quand même crée un Git pour que vous puissiez retrouver nos traces, ainsi que les différents éléments qui nous ont permis de répondre aux questions (capture, certificats, ...). Pour certaine réponse, nous avons ajouté des références clairement, faisant référence aux preuves de notre analyse. Le lien du Github est le suivant:https://github.com/louisbau/ReseauProjet

III. DNS

A. Combien de noms de domaines sont résolus et quand ?

Globalement, les requêtes DNS sont lancées à chaque fois que l'application a besoin d'accéder à un nouveau serveur. Par exemple, lors du lancement de l'application, plusieurs requêtes DNS sont faites. Il y a également des requêtes DNS envoyées lorsqu'on créer un meeting. Certaines fonctionnalités de l'application nécessitent également des requêtes DNS notamment la création d'un tableau blanc.

À chacune de ces étapes, environ 5 noms de domaine sont résolus.

B. Quels sont les serveurs autoritatifs pour ces noms de domaines ? Sont-ils gérés par des entreprises différentes ?

Tous les serveurs autoritatifs des différents noms de domaines sont gérés par une seule et même entreprise : Amazon. Cette affirmation est dûe à plus d'une dizaine de noms de domaine résolus manuellement via l'outils dig.

C. À quelles entreprises appartiennent les noms de domaines résolus ? Il y en a-t-il d'autres que celle qui détient l'application ?

Les noms de domaines résolus appartiennent tous à Zoom, c'est à dire à l'entreprise qui détient l'application. Aucun nom de domaine résolu n'appartient à une autre entreprise que Zoom.

D. Quels sont les types de requête DNS effectuées ?

Il y a plusieurs types de requête DNS effectuées. Tout d'abord il y a des requêtes DNS A pour rechercher des adresses IPV4. Ensuite, il y a des requêtes AAAA pour rechercher une adresse IPV6. Il y a également des recherches CNAME pour trouver l'adresse via un alias.

E. 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 ?

L'application reçoit des adresses IPV4 ainsi que IPV6. Zoom reçoit autant d'adresses IPV4 que d'adresses IPV6. Il n'y a donc pas de version IP préférée par l'application. Au vu des requêtes DNS IPV4 et IPV6 très rapprochées dans les traces Wireshark, on dirait que Zoom fait une requête A ainsi que AAAA à chaque fois qu'il faut faire une requête DNS.

F. Les requêtes contiennent elles des records additionnels ? Le cas échéant, à quoi servent-ils ?

Les requêtes DNS contiennent souvent un record additionnel. Ce record additionnel est utile pour augmenter la sécurité des requêtes DNS (OPT). Ces sécurités s'appellent DNSSEC cf. [3] .

G. Observez-vous des comportements DNS inattendus ?

Nous n'avons pas remarqué de comportements DNS étranges ou inattendus.

IV. Couche réseau

A. Lorsque IPv4 est utilisé, l'application utilise-t-elle des techniques pour traverser les NAT

Oui, l'application Zoom utilise des techniques pour traverser la NAT en IPv4, elle utilise les 3 techniques principalement utilisées : STUN, TURN et ICE.

STUN va être utilisé pour permet aux utilisateurs de communiquer directement avec les serveurs de Zoom plutôt que de passer par des serveurs relais.

ICE utilise STUN et d'autres protocoles pour permettre une communication en temps réel entre les clients de Zoom.

TURN est un protocole utilisé lorsque la communication directe entre les utilisateurs de Zoom n'est pas possible en raison du pare-feu ou des restrictions lier au NAT.

Remarque, l'utilisation des filtres turn, ice et stun ne permettent pas de le voir directement la présence des paquets utilisant ces techniques, une analyse des adresses et ports a dû être faite pour le confirmer .

B. 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 ?

Les adresses utilisées pour envoyer les paquets sont les suivantes : 192.168.1.1 , 127.0.0.53, 127.0.0.1, 10.0.2.15 ... . Dont la tendance des noms domaines correspondant à ".zoom.us" (cf. [4]). Quelque exemple: us05web.zoom.us, us04zpns.zoom.us ou encore us04xmppapi.zoom.us.

Nous pouvons observer que Zoom utilise des adresses Ip privées pour la NAT car elles permettent de réduire drastiquement les coût et la complexité du réseau, tout en permettant de traverser la NAT. L'utilisation d'adresse privé indique que des techniques pour traverser la NAT sont utilisé et confirme donc la présence de technique comme STUN, TURN et ICE.

V. Couche transport

A. Quels sont les protocoles de transports utilisés pour chaque fonctionnalité ?

La création d'une réunion se passe majoritairement sous le protocole TCP. L'envoi de messages textuels se déroule également selon le protocole TCP tandis que la transmission de messages audios (avec le micro) ainsi que la transmission de flux vidéo (caméra) se déroulent tous deux via le protocole UDP. La création de tableau blanc utilise les protocoles TCP et UDP.

Nous pensons que l'envoi de message textuel utilise le protocole TCP parce qu'il faut être sûr que le message de l'utilisateur ne soit pas altéré par le passage des paquets sur le réseau et que l'envoi de message textuel n'est pas une fonctionnalité qui nécessite beaucoup d'appels réseaux. Utiliser le protocole TCP ne va dont pas impacter les performances de l'application.

Le fait que les messages audio ainsi que la transmission de flux vidéo utilisent tous deux le protocole UDP est parce que ces deux fonctionnalités font énormément d'envois sur le réseau. Zoom accepte le fait de prendre plus de risques d'erreurs car utiliser le protocole TCP pour ces fonctionnalités entraînerait des problèmes de performances.

B. Il y a-t-il plusieurs connexions vers un même nom de domaine ? Si oui, pouvez-vous l'expliquer ?

Il y a effectivement plusieurs connexions vers un même nom de domaine. Nous pensons que ces différentes connexions sont dues au fait que les connexions démarrées entre le serveur et le client ne sont pas conservées très longtemps. Il faut donc renouveler les connexions lorsque le client a besoin de contacter le serveur.

C. Si vous observez du trafic QUIC, quels sont les versions utilisées ? Pouvez-vous identifier des extensions négociées dans le handshake ?

Nous n'avons pas observé de trafic QUIC lors de nos tests.

D. Lorsque vous observez du trafic UDP, identifiez-vous d'autres protocoles que QUIC et DNS ? Expliquez comment ils sont utilisés par l'application.

Lorsqu'on reste dans une réunion sans rien faire de particulier et que l'on observe du trafic UDP, on peut également souvent observer du trafic WireGuard. Ce protocole permet de créer un réseau virtuel privé (VPN) et est effectivement transmis grâce au protocole UDP.

Nous n'avons pas remarqué d'autres protocoles hormis WireGuard.

VI. Chiffrement et sécurité

A. L'utilisation du DNS est-elle sécurisée ? Comment ?

Oui l'utilisation du DNS sur Zoom est sécurisée. Et cela est possible grâce à l'utilisation du DNSSEC qui permet de garantir l'authentification et l'intégrité des réponses DNS et encore par l'utilisation des protocole DoT et DoH qui permette d'éviter qu'une personne malveillante ce trouve dans le réseau (man-in-the-middle).

B. Quelles versions de TLS sont utilisées ? Précisez les protocoles de transport sécurisés par ces versions.

Les versions utilisées pour TLS par Zoom sont les suivantes:

- TLSv1.3
- TLSv1.2

Pour TLSv1.2, les protocoles de transport sécurisé sont:

- Hypertext Transfer Protocole
- Handshake
- change Cipher Spec

Et pour TLSv1.3, les protocoles de transport sécurisé sont:

- Handshake
- change Cipher Spec
- Hypertext Transfer Protocole

C. Quel est la durée de vie des certificats utilisés ? Par qui sont-ils certifiés ?

La durée de vie des certificats utilisés par Zoom est de 1 ans et sont certifié par DigiCert, si on télécharge (cf. [6]) les différents certificats on peut constater qu'ils sont délivrés par DigiCert TLS RSA SHA256 2020 CA1. (cf. [7])

D. Lorsque vous pouvez observer l'établissement du chiffrement, quels sont les algorithmes de chiffrement utilisés ?

L'utilisation de End-To-End Encryption est faite pour effectuer le chiffrement sur l'application Zoom. Comme par exemple, AES 256 bits pour le chiffrement des données et RSA 2048 bits pour les échanges de clé (ou RSA 3072 bits). (cf. [8])

E. Si vous observez du trafic UDP, semble-t-il chiffré ? Comment est-il sécurisé ?

Oui, le trafic UDP est chiffré à l'aide de AES en mode Galois Counter. On le constate clairement sur les différentes trace découverte.

VII. Application

A. Quels comportements observez-vous lors d'une conversation comparée à un appel ? Quel impact à l'utilisation de la vidéo par rapport à un appel audio uniquement ?

L'impact de l'utilisation de la vidéo est beaucoup plus important que celle de l'utilisation d'un appel audio car il est essentiel pour zoom de fournir un service de qualité lors d'un appel quelconque, et donc de devoir synchronisé la voix ainsi que la vidéo entre elle en temps réel. Et par conséquent un nombre plus grand de trace est échanger au niveaux des appels vidéo.

B. 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).

Nous avons calculé pour les différentes applications les valeurs suivantes:

- Pour un appel audio et vidéo, Zoom utilise environ 9 Mo par minute de donnée échangées. (cf. [9])
- Pour un appel audio uniquement, Zoom utilise environ 0,4 Mo par minute de donnée échangées.
- Pour un appel vidéo uniquement (sans audio), Zoom utilise environ 9 Mo par minute de donnée échangées.
- Pour un appel vidéo avec le partage d'écran activé (sans audio), Zoom utilise environ 14 Mo par minute de donnée échangées.

Nous avons pu calculer ça grâce à Wireshark avec un filtre globale des connexion établies par utilisateur et les propriétés de la capture. Il nous a suffi de convertir en seconde les informations données par Wireshark.

C. l y a-t-il des serveurs relais utilisés pour interagir avec un utilisateur ou les applications communiquent-elles directement ? Observez-vous autre chose lorsque les deux utilisateurs sont sur le même réseau WiFi ?

Comme nous avons vu plus haut, Zoom utilise des techniques des pour traverser le NAT et ces techniques permettent d'éviter interagir avec des utilisateurs en temps réel à l'aide de communication direct ou par serveur relais. Par conséquence, sauf rare exception, exemple sur le réseau Eduroam, nous ne pensons pas que l'application utilise souvent des serveur relais. Nous ne parvenons pas à observer d'autres éléments lorsque les deux utilisateurs sont sur le même réseau WiFi. Mais nous imaginons bien que la technique ICE doit avoir un impact sur les traces envoyées car les utilisateurs peuvent communiquer directement sans serveur relais.

D. Est-ce qu'interagir avec un utilisateur se trouvant dans le même réseau Wi-Fi ou Ethernet à un impact sur la façon dont le trafic applicatif est transporté ? Il y a-t-il des serveurs relais ?

Pour cette question, nous pensons qu'il n'y pas de serveurs relais lorsqu'on se trouve sur un même réseau et que la technique ICE est utilisé dans ce cas si. Et donc oui il y a un impact. Cependant nous n'avons pas su examiner analyser correctement pour répondre définitivement à la question.

VIII. Conclusion

Pour conclure notre travail, nous pensons avoir répondu au but premier du projet, pouvoir comprendre le fonctionnement des Protocoles qui constituent l'Internet et également le comportement de ses applications. Nous avons aussi approfondi nos connaissances vis à vis de l'outil Wireshark, l'utilisation de filtre ainsi que les différentes fonctionnalités implémentées.

References

[1] Introduction à l'analyse réseau avec Wireshark. (2014, 19 septembre). Developpez.com. https://inetdoc.developpez.com/tutoriels/analyse-reseau-wireshark/
[2] https://github.com/louisbau/ReseauProjet/blob/main/README.md
[3] https://github.com/louisbau/ReseauProjet/blob/main/Capture/additionalRecord.PNG
[4] https://github.com/louisbau/ReseauProjet/blob/main/Capture/domaineTendance.PNG
[5] https://github.com/louisbau/ReseauProjet/blob/main/Capture/protcoleTLS.PNG
[6] Atkin, R. (2022, 15 janvier). Identifying and retrieving TLS/SSL Certificates from a PCAP file using Wireshark. https://richardatkin.com/post/2022/01/15/Identifying-and-retrieving-certificates-from-a-PCAP-file-using-Wireshark.html
[7] https://github.com/louisbau/ReseauProjet/blob/main/certificat/cert.cer
[8] https://github.com/louisbau/ReseauProjet/blob/main/Capture/chiffrement.PNG
[9] https://github.com/louisbau/ReseauProjet/blob/main/Capture/donneeEchange.PNG