Analyse de l'application Whatsapp

Tristan Richard 15552000 Louis Viaene 43111900

***Abstract*—Ce document est le rapport d'analyse des différents protocole réseau de l'application Whatsapp**

I. Introduction

En tant qu'ingénieur 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 ingénieur réseau peut à la fois améliorer les protocoles de l'Internet et concevoir des applications réseaux efficaces. Ainsi, dans le cadre du cours LEPL1341- réseau informatique, nous avons analysé le fonctionnement réseau de l'application Whatsapp.

II. Présentation de l'application

WhatsApp web est une application de messagerie instantanée en ligne qui permet aux utilisateurs de WhatsApp de se connecter à leur compte WhatsApp via un navigateur Web. Elle offre une grande variété de fonctionnalités, telles que la messagerie, les appels vocaux et vidéo, ainsi que la possibilité de partager des fichiers tels que des photos, des vidéos et des documents. L'application permet également de créer des groupes de discussion.

III. Protocole de Test

Dans l'objectif d'analyser toutes les fonctionnalités réseaux de l'application, nous avons convenu d'un protocole de test. Tout d'abord, aucune autre application ne doit être éxécutée pour éviter tout flux autre que celui de whatsapp. Voici la liste des actions réalisées dans l'ordre chronologique:[1]

- ouvrir l'application
- envoyer un message
- envoyer un fichier
- réaliser un appel vocal
- réaliser un appel vidéo

IV. Domain Name System

Le Domain name system aussi appelé DNS est un système qui permet de traduire des noms de domaine en adresses IP numérique compréhensible par les ordinateurs. On peut le comparer à un annuaire téléphonique pour Internet

[1]les captures sont disponibles sur le git [1]

A. Noms de domaines résolus

La capture Wireshark [2] a révélé que huit noms de domaines ont été résolus par l'application WhatsApp. Deux de ces noms de domaines ont été résolus au début de la capture, quatre autres à 24 secondes , deux autres à 25 secondes et enfin deux autres à 26 secondes.

TABLE I
ANALYSE DNS

Nom de domaine	IPv4	IPv6
g.whatsapp.net	179.60.195.49	non
e2.whatsapp.net	15.197.206.217	non
mmg.whatsapp.net	179.60.195.51	oui
media-bru2-1.cdn.whatsapp.net	179.60.195.51	oui
media-ams4-1.cdn.whatsapp.net	157.240.201.60	oui
media.fbru5-1.fna.whatsapp.net	194.78.99.162	oui
wpad.home		
wpad.home		
x1.c.lencr.org	23.52.55.67	oui

Pour la deuxième demande, e2.whatsapp.net, nous avons remarqué que l'on recoit plusieurs adresses IPv4 pour une seule demande. Cela est du au DNS qui répartit le flux sur plusieurs serveurs pour diviser le trafic. [3]

B. Entreprise

A l'aide des résultats de l'analyse DNS et au site web Whois [4], nous observons que les noms de domaines résolus n'appartiennent pas seulement à whatsapp mais à plusieurs entreprises différentes, notamment Latin American and Caribbean IP address Regional Registry (LACNIC), Amazon, Meta et Akamai. Meta est la société propriétaire de whatsapp, amazon est le leader mondiale en terme d'infrastructure réseau et Akamai est une société qui heberge le cache.

C. Type de requêtes

- SOA: permet de récupérer les infos importantes sur un domaine
- CNAME: Fait correspondre le nom de domaine alternatif au nom de domaine réel
- A: permet de trouver l'adresse IPv4
- AAAA: permet de trouver l'adresse IPv6

D. Famille d'adresse IP

L'application a utilisé à la fois IPv4 et IPv6 pour toutes les requêtes DNS. L'IPv4 est l'adresse IP la plus couramment utilisée, mais il y a de plus en plus de serveurs qui prennent en charge l'IPv6 pour améliorer la sécurité et la fiabilité. Si

on ne demande que l'IPv4 et que le serveur ne prend en charge que l'IPv6, la connexion ne peut pas être établie. En demandant à la fois l'IPv4 et l'IPv6, on peut s'assurer qu'il peut se connecter au serveur quelle que soit l'adresse IP prise en charge.

E. Conclusion

L'analyse DNS a permis de comprendre les noms de domaines utilisés par l'application WhatsApp, les serveurs autoritaires pour ces noms de domaines, les entreprises à qui appartiennent les noms de domaines résolus, les types de requêtes DNS effectuées et la famille d'adresse IP préférée. L'analyse n'a révélée aucune requêtes contenant des records additionnels ni de comportement inattendu.

V. Couche réseau

A. Procédure

Pour réaliser l'analyse des échanges de paquets, nous avons réalise un script python[2] qui analyse automatiquement les adresses de destinations les plus fréquentes, traduit ces adresses IP en leurs noms de domaine et les réprésentent avec un graphe pour permettre une analyse plus simple.

B. Analyse

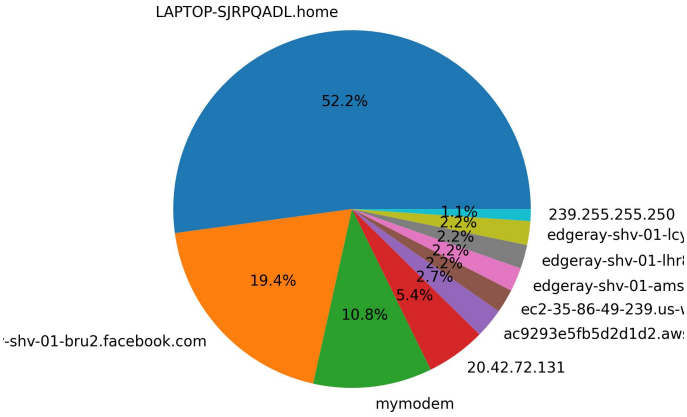

Fig. 1. analyse des destinations les plus fréquentes

Remarquons que la majorité des paquets ont pour destination LAPTOP-SJRPQADL.home. Cela s'explique aisément, car cette adresse correspond à mon ordinateur personnel, utilisé pour effectuer les tests. Ainsi, il reçoit naturellement des paquets provenant des serveurs WhatsApp.
10% des paquets sont eux en direction de mymodem, cela est dû au fait que toutes les connexions Internet passent par le modem, qui agit en tant que passerelle pour les périphériques connectés au réseau. Par conséquent, chaque fois qu'un périphérique effectue une connexion sortante vers Internet, l'adresse IP de destination sera celle de la passerelle.

[2]disponible sur le github [1]

20% sont dirigé vers ce nom de domaine: -shv-01-bru2.facebook.com, c'est un serveur appartenant à facebook. C'est donc totalement normal étant donné que whatsapp appartient à facebook.

C. NAT

Dans le cadre de l'analyse de l'utilisation des protocoles réseau, nous avons observé des échanges de requêtes STUN dans les captures Wireshark. Ces requetes rentrent dans le cas d'utilisation de NAT.
Les NAT sont souvent utilisés dans les réseaux pour partager une adresse IP publique entre plusieurs hôtes. Les NAT sont souvent configurés de manière à bloquer les connexions entrantes qui n'ont pas été initiées par un hôte interne. Cela peut poser des problèmes pour la communication entre deux hôtes situés derrière des NAT différents. Les requêtes STUN permettent alors de contourner ces problèmes en découvrant l'adresse IP publique et le port associé du NAT, et en utilisant ces informations pour configurer les sessions de communication. [5]

D. Conclusion

Nous avons remarqué que la majorité des paquets sont en direction de l'ordinateur personnel et qu'un serveur facebook est fréquemment contacté, nous avons également pu remarquer des requetes STUN qui ont pour objéctif de traverser les NAT.

VI. Couche transport

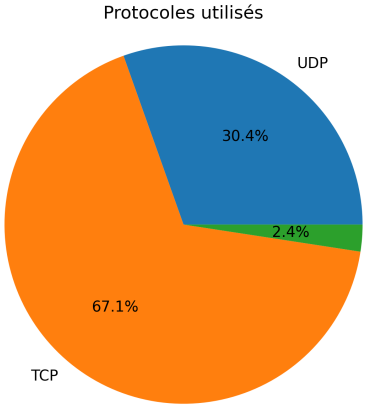

Fig. 2. analyse des protocoles de transport

En observant les protocoles de transport utilisés, on remarque que plus d'un tiers sont de type TCP. Ce protocole est préféré en raison de sa fiabilité et de sa capacité à minimiser les pertes de données. Cependant, une analyse plus approfondie avec Wireshark montre que le protocole UDP est principalement utilisé pour les appels vers la fin de la capture. Bien qu'il soit plus rapide que TCP, il est moins fiable, ce qui peut expliquer cette utilisation sélective. Nous ne detectons aucun quic lors de l'analyse wireshark. [6]

VII. CHIFFREMENT ET SÉCURITÉ

Avec l'analyse de paquets, on remarque que l'application whatsapp utilise à la fois des certificats TLSv1.2 et TLSv1.3 pour permettre un plus grande compatibilité.

A. echange

On observe que le client envoie régulièrement des demande ClientHello et recoit des reponses ServerHello, ces échanges permettent de décider des options de connexion. On remarque que la réponse ServerHello fournit à chaque fois la meme cipher suite

B. cipher

La cipher suite utilisé est :TLS_AES_128_GCM_SHA256. Cette cipher suite utilise une clé de session de 128 bits, qui est générée pour chaque nouvelle connexion TLS, pour éviter la réutilisation des clés et augmenter la sécurité.
Cette suite utilise l'algorithme de chiffrement symétrique AES 128 bits en mode de chiffrement GCM. GCM est considéré comme l'un des modes les plus sûrs pour les communications sécurisées sur Internet car il offre des avantages en termes de sécurité, de vitesse et d'efficacité. En particulier, il permet de réaliser le chiffrement et l'authentification des données en même temps, ce qui permet de réduire le temps de traitement et de minimiser les risques d'attaques.[3]. Finalement, la fonction de hashage SHA-256 est utilisé pour calculer les empreintes de hachage des messages TLS pour garantir leur intégrité et leur authenticité, la cipher suite "TLS_AES_128_GCM_SHA256" est considérée comme sûre et efficace pour les échanges de données en ligne et est couramment utilisée dans les implémentations TLS modernes. [7] [8]

C. option

On remarque dans les echanges TCP que les options négociés sont:

- maximum segment size: 1452bits
- window scale: 8
- SACK permitted

La maximum segment size est la plus grande taille de données que le destinataire peut accepter en une seule fois. Le "window scale" permet d'augmenter la taille de la fenêtre de réception pour améliorer le débit. SACK permet au destinataire d'indiquer quels segments ont été reçus avec succès, ce qui permet de récupérer plus rapidement les données manquantes en cas de perte de paquets.

D. flag

L'analyse du trafic réseau a permis de relever l'utilisation des flags TCP suivants lors des échanges observés :

- SYN : ce flag est utilisé pour initier une connexion TCP
- ACK : ce flag est utilisé pour confirmer la réception de segments TCP
- FIN : ce flag est utilisé pour indiquer la fin d'une communication TCP
- PSH : ce flag est utilisé pour indiquer que les données doivent être transmises immédiatement au destinataire sans attendre d'autres segments

[3]mettre une référence

E. Conclusion

En conclusion, l'analyse de paquets de l'application WhatsApp a permis de mettre en évidence l'utilisation de certificats TLSv1.2 et TLSv1.3 pour assurer une communication sécurisée entre les clients. Les échanges ClientHello et ServerHello ont permis de négocier la cipher suite "TLS_AES_128_GCM_SHA256", qui utilise l'algorithme de chiffrement symétrique AES 128 bits en mode de chiffrement GCM, offrant une sécurité accrue et une efficacité optimale pour les communications en ligne. Les options de négociation TCP, telles que le maximum segment size, le window scale et SACK, ont été utilisées pour optimiser les performances du réseau et réduire les pertes de données. Les flags TCP tels que SYN, ACK, FIN et PSH ont été utilisés pour initier, confirmer et terminer les communications TCP. Dans l'ensemble, l'utilisation de ces technologies de sécurité et de communication dans l'application WhatsApp assure une expérience utilisateur sécurisée et efficace. Aucune faille de sécurité n'a été découverte.

VIII. APPLICATION

A. impact sur le trafic

la quantité de trafic réseau utilisé pour un appel ou un message n'est pas la même. En effet, lors d'un appel vocal qui est estimé a 500 ko pour une minute, on observe une augmentation significative du trafic réseau par rapport a un message. celui-ci ne demande pas beaucoup de charge reseau du fait que la quantité de donnée envoyé est faible, on parle ici de l'ordre de 1 ko. A contrario, un appel video demande une charge réseau beaucoup plus importante du fait de du volume de données échangées en continu, nous avons ici une estimation de 6 Mo par minute.

REFERENCES

[1] github: https://github.com/tristanrichard/projet_linfo1341
[2] Wireshark : https://www.wireshark.org/
[3] "Load balancer : pour un meilleur temps d'accès au serveur." IONOS, 09.02.23,https://www.ionos.fr/digitalguide/serveur/know-how/load-balancer-repartition-de-charge-sur-un-serveur/
[4] Whois: https://who.is/
[5] "Comprendre la NAT pour activer la communication peer-to-peer sur les routeurs IOS et IOS XE." CISCO, 07.12.22, https://www.cisco.com/c/fr_ca/support/docs/ip/network-address-translation-nat/217599-understand-nat-to-enable-peer-to-peer-co.html
[6] Guipelbé, Adam. "Différence entre TCP et UDP" Dirtech, https://www.dir-tech.com/difference-entre-tcp-et-udp/
[7] "AES GCM Encryption Algorithms", https://vocal.com/cryptography/gcm-and-gmac-authenticated-encryption-algorithms/
[8] Ayala, Gabriel. "Qu'est-ce que SHA-256?" bit2me academy, 23.07.18, https://academy.bit2me.com/fr/sha256-algoritmo-bitcoin/