Analyse de l'application Whatsapp

Tristan Richard 15552000

***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

A. Noms de domaines résolus

La capture Wireshark 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

B. Entreprise

A l'aide des résultats de l'analyse DNS et au site web Whois, 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

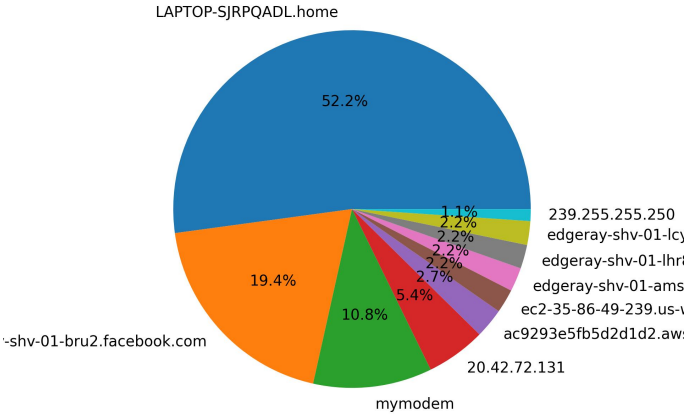

Fig. 1. analyse des destinations les plus fréquentes

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

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.

VI. Couche transport

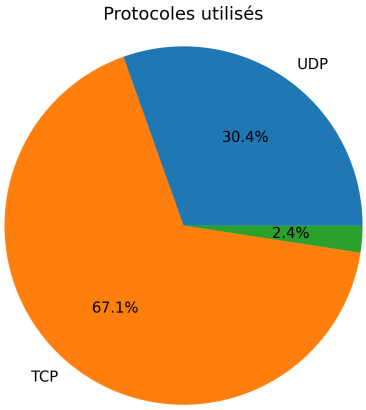

Fig. 2. analyse des protocoles de transport

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.

REFERENCES

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.