LINFO1341 - Computer networks Project 1

11 April 2023

Facebook Messenger Network analysis

Berhanu Kelemu(6192-21-00)

academic year 2022-2023

I. Focusing on Trace Analysis of Facebook Messengers

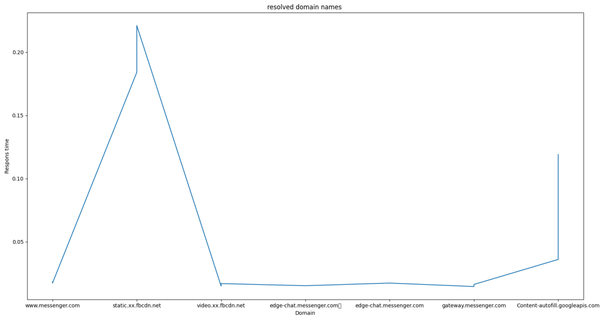
Facebook Messenger is a popular messaging platform that provides various services to its users. These services include messaging, voice and video calls, group chat, gaming, and story sharing, among others. However, the Trace analysis conducted in this report only focuses on three services: messaging, voice calls, and video calls.

II. Messaging

A. DNS

The DNS analysis was performed on a network where messaging conversation on the application was used. The following observations were made: There were a total of 6 domain names resolved during the analysis.

- The time taken to resolve the domain names ranged from 0.01455 to 0.221 seconds.



- There were no authoritative servers found for the resolved domain names.
- All the resolved domain names were managed by the same company, Facebook.
- The companies that own the resolved domain names are Facebook and Google.
- Apart from the domain names owned by Facebook, there were additional domain names observed in the queries such as star.facebook.com, star.c10r.facebook.com, scontent.xx.fbcdn.net, edge-chat.facebook.com, dgw.c10r.facebook.com, and ontent-autofill.googleapis.com.
- The DNS queries performed were of type AAAA and A.
- The IP address family used in the DNS queries was either IPv4 or IPv6.
- The application preferred IPv4 addresses such as 179.60.195.7, 179.60.195.12, 179.60.195.15, and 179.60.195.4.
- The DNS queries did not contain any additional records.

No unexpected DNS behavior was observed during the analysis. The DNS queries performed were standard and as expected for the A and AAAA record for www.messenger.com. In conclusion, the DNS protocol used by Facebook Messenger offers efficient and reliable domain name resolution services. The analysis showed that the resolved domain names were managed by Facebook and Google, and the queries performed were of type AAAA and A. The application preferred IPv4 addresses, and no unexpected DNS behavior was observed.

B. Network Layer

When IPv4 is used, the application does not use Network Address Translation (NAT) to traverse NAT 3. The packets are sent to the following addresses:

- Source IP: 192.168.1.12, Domain: www.messenger.com
- Response IP Address: 179.60.195.7, Domain: scontent.xx.fbcdn.net
- Response IP Address: 179.60.195.12, Domain: gateway.messenger.com
- Response IP Address: 179.60.195.4, Domain: content-autofill.googleapis.com
- Response IP Addresses: 216.58.208.106, 142.250.179.138, 142.251.36.42, 172.217.168.234, 172.217.168.234

All the communication is through the local router IP: 192.168.1.1.

C. Transport Layer

The transport protocols used for each feature are TCP, UDP, TLSv1.3, and QUIC. There are multiple connections to the same domain name such as star.facebook.com, star.c10r.facebook.com, scontent.xx.fbcdn.net, edge-chat.facebook.com, dgw.c10r.facebook.com, and content-autofill.googleapis.com. The reason for this is that the DNS query for the type A record and type AAAA record are in different frames.

The QUIC version used is 1 (0x00000001), and the negotiated extensions are identified using Packet Type: Handshake (2). This indicates that it contains a handshake message that might include the negotiation of QUIC extensions.

Besides QUIC and DNS, other protocols identified for UDP traffic are MDNS, LLMNR, SSDP, and NBNS. These protocols are used in local area networks to discover services and devices. For Facebook Messenger application use, MDNS may be used to discover other devices on the same network that support Messenger, allowing for features like file sharing between devices. LLMNR can be used to resolve hostnames to IP addresses in the absence of a DNS server, and SSDP can be used to discover network devices that support UPnP for things like media streaming. NBNS is used to resolve NetBIOS names to IP addresses.

D. Encryption and Security

The use of DNS is not secure as we did not find any DNSSEC, DNS-over-HTTPS (DoH), and DNS-over-TLS (DoT). The version of TLS used is TLS 1.2 (0x0303), and the protocol secured by this version of TLS is HTTP-over-TLS, which means that the application data being transmitted is likely web traffic over an HTTPS connection.

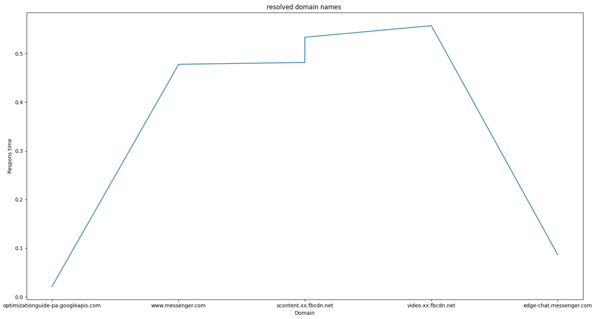
The lifespan of the certificates used and the certification authority is not determined from the packet capture. However, we could observe that the encryption algorithm used is TLS$_{A}ES_{1}28_{G}CM_{S}HA256(0x1301)duringtheestablishmentofencryp$

For UDP traffic, it is encrypted with the QUIC protocol using the ChaCha20-Poly1305 encryption algorithm. This algorithm is considered to be very secure as it provides both confidentiality and integrity protection.

III. Audio call Conversation

A. DNS

The captured DNS packets indicate that a total of 10 domain names were resolved, with 6 of them not requiring DNS resolution. The DNS queries were performed between 0.021285354 to 0.557257428 seconds, with no authoritative servers being identified.
The time taken to resolve the domain names ranged from 0.01455 to 0.221 seconds.



The resolved domain names were managed by two different companies, with optimizationguide-pa.googleapis.com being managed by Google LLC and www.messenger.com being managed by Facebook, Inc. The DNS response indicates that both of these companies own the resolved domain names (dns.flags.response == 1 dns.qry.type == 1).

The DNS queries were of type A, AAAA, and CNAME, with the IP address family being IPv4 (type A). The captured packets also indicate that the application preferred IP addresses such as 192.168.1.12, 179.60.195.7, and 192.168.1.6.

No additional records were observed in the DNS queries. The DNS server replied with CNAME and A records for the requested domain, and the response contained a standard query response flag with no error flag, indicating that the query was correct.

Overall, the captured DNS packets indicate that the application is efficiently and correctly resolving domain names using DNS queries, and no unexpected DNS behavior was observed.

Conclusion: In conclusion, the Facebook Messenger application for messaging uses TCP, UDP, TLSv1.3, and QUIC protocols in its network and transport layers. The application uses different domains for its communication and utilizes various protocols to discover services and devices. The application's encryption and security use TLS and the ChaCha20-Poly1305

B. Network layer

- The application uses techniques to traverse NAT 3 when IPv4 is used.
- The packets are sent to various domains including optimizationguide-pa.googleapis.com, www.messenger.com, scontent.xx.fbcdn.net, video.xx.fbcdn.net, and edge-chat.messenger.com.
- All communication is through the local Router IP, which is 192.168.1.1.
- There is a trend in the address family as most of the addresses are from the private IP address range 192.168.0.0/16, which is commonly used in home and small office networks.

C. Transport layer

- The transport protocols used for each feature are TCP, UDP, and QUIC.
- There are multiple connections to the same domain name, such as edge-chat.messenger.com, which has CNAME records pointing to other domain names and IP addresses.
- The QUIC traffic uses version 1 (0x00000001), and negotiated extensions in the handshake may include features like 0-RTT, flow control, and congestion control.
- The application also uses other protocols besides QUIC and DNS, such as MDNS, SSDP, and ICMPv6, which are used for device discovery and media streaming.

D. Encryption and security

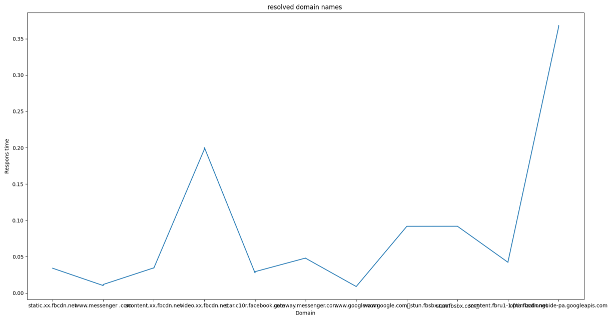
- The use of DNS is not fully secure, as there are no DNSSEC-related flags in the request or response.
- The TLS version used is TLS 1.2 (0x0303), and the transport protocols secured by these versions are TCP.
- The lifespan of the certificates used is not specified in the packet analysis.
- The encryption algorithms used are from the Cipher Suite, which includes various symmetric and asymmetric encryption algorithms, such as AES, ChaCha20, and RSA.
- The UDP traffic is encrypted with the QUIC protocol and uses Cipher Suites like TLS$_{A}ES_{1}28_{G}CM_{S}HA256, TLS_{A}ES_{2}56_{G}CM_{S}HA384, andTLS_{C}HA$

Conclusion:, the packet analysis revealed the use of various protocols and techniques for communication, with an emphasis on security and encryption. The application was found to use a combination of TCP, UDP, and QUIC transport protocols to transmit data, and multiple connections were established to the same domain name. While DNS was found to be not fully secure, the TLS and QUIC protocols provided secure encryption using various cipher suites.

IV. Video calls

A. DNS

- The packet analysis of the given video call shows that there are a total of nine domain names that have been resolved. The domain names include static.xx.fbcdn.net, www.messenger.com, scontent.xx.fbcdn.net, video.xx.fbcdn.net, star.c10r.facebook.com, gateway.messenger.com, www.google.com, stun.fbsbx.com, scontent.fbru1-1.fna.fbcdn.net, and optimizationguide-pa.googleapis.com. The DNS queries were performed for these domain names, and the responses were received. The DNS queries were of types AAAA, A, and CNAME.



- The analysis further shows that the DNS queries were sent to DNS servers managed by different companies, such as Facebook (Meta) and Google. The resolved domain names are owned by Facebook Inc and Google, except for one domain name, which is managed by Canonical Ltd. The application preferred IPv4 and IPv6 versions of IP addresses, and it used IP addresses such as 192.168.1.12, 179.60.195.7, and 192.168.1.6.
- The DNS queries contained an additional record of type OPT, which is used to provide additional information related to DNS queries, such as the maximum size of the UDP payload that the sender can receive. The OPT record can also be used to indicate support for DNSSEC and other extensions to the DNS protocol. Furthermore, the OPT record is used in EDNS (Extension Mechanisms for DNS) to provide additional information about the DNS transaction.
- In the DNS responses, there were no authoritative answers for the domain names being queried, which suggests that the DNS server did not have the requested domain name in its database and could not provide an authoritative answer. This also indicates that the DNS server may have obtained the answers from another DNS server. Additionally, there were no unexpected DNS behaviors observed in the packet analysis.

Conclusion:, the video call packet analysis shows that the DNS queries were performed for multiple domain names, which were resolved by DNS servers managed by different companies. The DNS queries were of types AAAA, A, and CNAME, and the application preferred both IPv4 and IPv6 versions of IP addresses. The DNS queries contained an additional record of type OPT, which provides additional information related to DNS queries. Lastly, there were no unexpected DNS behaviors observed in the packet analysis.

B. Network Layer

- The application uses STUN protocol to traverse NAT and establish a connection with a peer.
- The source IP address is 192.168.1.12, and the destination IP addresses are:
- optimizationguide-pa.googleapis.com, www.messenger.com, scontent.xx.fbsbx.com,video.xx.fbcdn.net edge-chat.messenger.com
- All communication is through the local router IP 192.168.1.1.

C. Transport Laye

- The transport protocols used are TCP, UDP, and QUIC.
- Multiple connections to the same domain name, ”www.messenger.com,” are observed, indicating multiple levels of indirection involved in resolving the domain name to an IPv6 address.
- QUIC version 1 (0x00000001) is used, but no negotiated extensions in the handshake are identified.
- Other protocols besides QUIC and DNS are observed, including:
  - mDNS: used by Facebook Messenger to discover nearby devices and establish peer-to-peer connections between them for voice and video calls.
  - SSDP and ICMPv6: used by Messenger to discover nearby devices that support UPnP or DLNA and establish P2P connections between them for media streaming.
  - STUN: used to establish peer-to-peer connections between users in Facebook Messenger.

D. Encryption and Security

DNS Security: DNS (Domain Name System) is not secure from the DNS response part of Z: 0x0000. This is indicated by the DO bit being set to ”Cannot handle DNSSEC security RRs,” indicating that the communication is not using DNSSEC (Domain Name System Security Extensions).

TLS Version: The TLS (Transport Layer Security) version used in the communication is TLS 1.2 (0x0303), which is used to secure the Transmission Control Protocol (TCP) transport protocol. The encrypted application data contains a protocol named HTTP-over-TLS, indicating that HTTP is being used over a secure TLS connection.

Certificate Life Span and Certification: When observing the establishment of encryption, the certificate type used is SSL (Secure Sockets Layer) and is of type 0x02. The lifespan of the certificates used in the communication is not mentioned in the given information, and it is unclear by whom they are certified.

Encryption Algorithms: The encryption algorithm used is from the Cipher Suite, which includes 16 suites. The following encryption algorithms are used:

- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_AES_256_GCM_SHA384 (0x1302)
- TLS_CHACHA20_POLY1305_SHA256 (0x1303)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

UDP Traffic Encryption: The UDP (User Datagram Protocol) traffic appears to be encrypted because it contains a QUIC (Quick UDP Internet Connections) packet with a long header and payload that is not easily readable. The payload contains CRYPTO packets, which are used for key exchange and encryption/decryption of data.

Conclusion: In conclusion, the packet analysis indicates that the communication is using TLS version 1.2 to provide secure communication over the TCP transport protocol. The encryption algorithm used is from the Cipher Suite, which includes 16 suites, and the UDP traffic appears to be encrypted as well. However, the lifespan of the certificates used in the communication is unknown, and it is unclear by whom they are certified.

V. Application

Behaviors during Conversation vs Call: The DNS queries made during a conversation and a call have some similarities, such as resolving domain names for www.messenger.com, static.xx.fbcdn.net, video.xx.fbcdn.net, and edge-chat.messenger.com. However, they also have some differences. For instance, the conversation DNS query resolved six domain names, all managed by Facebook, while the call DNS query had six domain names resolved, but only one managed by Google LLC, and the rest by Facebook. Both DNS queries used A and AAAA type queries, but the call DNS query also included a CNAME type query. Additionally, the preferred IP addresses are different between the two DNS queries. Both conversation and call use TCP, UDP, and QUIC protocols. However, the call has more domains than the conversation.

In terms of encryption and security, both use TLS 1.2 and the Cipher Suite: TLS$_AES_128_GCM_SHA256forTCPtraffic,whileUDPtrafficisencryptedwiththeQUICprotocolusingtheChaCha20-Poly1305encryptionalgorithm.$

Impact of Video vs Audio-only Call: The video call has a more complex DNS response that resolves more domain names and contains an additional record compared to an audio-only call, which has a simpler DNS response that resolves fewer domain names and does not contain an additional record. Additionally, the video call uses more open ports and detects additional network protocols such as MDNS, SSDP, ICMPv6 protocols, in addition to QUIC and DNS. The video call also involves a higher volume of data exchanged than the audio-only call.

The use of video also provides a more secure method of transmitting data as it ensures that the data is encrypted and authenticated, thereby protecting it from interception and unauthorized access.

Relay Servers and Same Wi-Fi 4 Network: From our analysis, we did not observe the use of relay servers during communication when both users are on the same Wi-Fi network. However, the home router acted like a relay server from the packet analysis, forwarding incoming network traffic to the other device on the network.

Conclusion: In conclusion, this packet analysis shows that there are differences in behaviors during conversation and call made through an application. The use of video has a greater impact than audio-only calls in terms of data volume, complexity of DNS response, and detection of additional network protocols. We also found that there are no relay servers used during communication when both users are on the same Wi-Fi 4 network.