Topics in Algebra: Cryptography

Univ.-Prof. Dr. Goulnara ARZHANTSEVA

WS 2018

Messaging security

Messaging Apps: WhatsApp, Snapchat, Facebook Messenger, Telegram, Viber, LINE and Skype, etc.

Types of protocols: HTTP + Push Notifications / Extensive Messaging and Presence Protocol (XMPP).

Two approaches to encryption: peer-to-peer encryption (P2P) / the end-to-end encryption (E2EE).

Protocols: the MTProto mobile protocol (Telegram), the Signal protocol (Open Whisper Systems).

Messaging security

Messaging Apps: WhatsApp, Snapchat, Facebook Messenger, Telegram, Viber, LINE and Skype, etc.

Types of protocols: HTTP + Push Notifications / Extensive Messaging and Presence Protocol (XMPP).

Two approaches to encryption: peer-to-peer encryption (P2P) / the end-to-end encryption (E2EE).

Protocols: the MTProto mobile protocol (Telegram), the Signal protocol (Open Whisper Systems).

Reference (again): Martin, K. M. Everyday cryptography. Fundamental principles and applications. Second edition. Oxford, 2017.

End-to-end encryption

The end-to-end encryption ensures that your message is turned into a secret message by its original sender (on sender's device), then only decoded by its final recipient (on recipient's device).

The Signal protocol is a non-federated cryptographic protocol that provides end-to-end encryption for voice calls, video calls, and instant messaging conversations.

The Signal protocol is used, for instance, by WhatsApp, Facebook Messenger, Google Allo and Signal's own messaging application.

WhatsApp security requirements

Confidentiality: The content is not accessible to anyone other than the communicating parties. In particular, the WhatsApp servers should not be able to decrypt messages.

Data origin authentication: Messages have not been modified by unauthorised parties.

Perfect forward secrecy: Compromise of any keys should not affect any previously transmitted messages.

WhatsApp cryptographic tools

Public-key pairs: Each user is associated with a large number of key pairs, which are used to establish shared secrets using the Diffie-Hellman protocol. These key pairs are all elliptic-curve-based ElGamal key pairs, generated using the elliptic curve Curve25519.

WhatsApp cryptographic tools

Public-key pairs: Each user is associated with a large number of key pairs, which are used to establish shared secrets using the Diffie-Hellman protocol. These key pairs are all elliptic-curve-based ElGamal key pairs, generated using the elliptic curve Curve25519.

Symmetric encryption: Messages are encrypted using AES-256 in the Cipher Block Chaining (CBC, 1976) mode. Each block of plaintext is XORed with the previous ciphertext block before being encrypted. So, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

WhatsApp cryptographic tools (suite)

Message authentication: Messages are accompanied by an hash-based message authentication code (HMAC, 1996) based on the hash function SHA-256.

Key derivation: Symmetric keys are derived using the HMAC-based extract-and-expand key derivation function (HKDF, 2010).

Initialising a WhatsApp session

Alice installs WhatsApp:

WhatsApp on Alice's device generates 3 public-key pairs

1. A long-term identity key pair (PK_A^{Id}, SK_A^{Id});
2. A medium-term signed pre-key pair (PK_A^{SP}, SK_A^{SP}) that is occasionally updated (signed by the identity key);
3. A list of one-time pre-key pairs $(PK_A^{OT_1}, SK_A^{OT_1}), \ldots, (PK_A^{OT_n}, SK_A^{OT_n})$ which are each used once and then discarded (a new list once all the key pairs are used).

Alice then submit the public keys $PK_A^{Id}, PK_A^{SP}, PK_A^{OT_1}, \ldots, PK_A^{OT_n}$ to the WhatsApp server for storage.

Only Alice's device knows the private keys.

Initialising a WhatsApp session

A session with Bob is initiated:

Establishment of a session:

1. Alice requests Bob's public keys PK_B^{Id}, PK_B^{SP}, $PK_B^{OT_i}$, (as $PK_B^{OT_1}, \ldots, PK_B^{OT_{i-1}}$ have been used and discarded by the server). Alice now knows three elliptic-curve-based ElGamal public-key values of Bob;

Initialising a WhatsApp session (suite)

Establishment of a session (suite):

2. Alice generates a fresh (ephemeral) one-time key pair (PK_A^*, SK_A^*) that is used to begin the session and then discarded. The shared secret can be computed (without direct communication): Alice can compute from PK_B and SK_A and Bob can compute it from PK_A and SK_B. They use the elliptic-curve Diffie-Hellman protocol (ECDH).

   Alice computes:

   (a) $MK_{AB}^1 = ECDH(PK_A^{Id}, PK_B^{SP})$;

   (b) $MK_{AB}^2 = ECDH(PK_A^*, PK_B^{Id})$;

   (c) $MK_{AB}^3 = ECDH(PK_A^*, PK_B^{SP})$;

   (d) $MK_{AB}^4 = ECDH(PK_A^*, PK_B^{OT_i})$;

Initialising a WhatsApp session (suite)

Establishment of a session (suite):

3. Alice concatenates the 4 shared secrets to form a shared master secret

$$M_{AB} = (MK^1_{AB}||MK^2_{AB}||MK^3_{AB}||MK^4_{AB}).$$

She uses the key derivation function HKDF to derive two shared 256-bit symmetric keys: a root key RK_{AB} and a chain key CK_{AB}.

4. When she send the 1st message of the new session to Bob, she includes her public keys PK^{Id}_A and PK^*_A. Using these values, Bob performs same computations as Alice in order to derive two symmetric keys RK_{AB} and CK_{AB}.

RK_{AB} is used to create CK_{AB}.

Deriving message keys

The keys to protect the messages are extracted from the message key MK_{AB}, a 640-bit value derived from the chain key CK_{AB} using HKDF.

The message key is then split into a 256-bit AES encryption key, a 256-bit HMAC-SHA-256 authentication key and a 128-bit IV for use in CBC mode.

Each message key is only used once to protect a single message from Alice to Bob.

A stored message key cannot be used to derive current or past values of the chain key.

Deriving message keys (suite)

Two mechanisms of the Signal protocol:

1. Each time a message key is derived, the chain key is updated to the result of computing HMAC-SHA-256 using the current chain key on a fixed constant input. So, the next message key is derived from a different chain key.
2. Each time a message is sent from Alice to Bob, Alice includes an ephemeral public-key PK_A^{update}. When she receives an answer from Bob (which includes PK_B^{update}), Alice computes $ECDH(PK_A^{update}, PK_B^{update})$ and then uses the key derivation function HKDF to derive new values for RK_{AB} and CK_{AB} from the result.

These two mechanisms ensure the perfect forward secrecy.
This is for the message from Alice to Bob. The replies from Bob to Alice require the generation of separate sets of keys.

WhatsApp's messaging: summary

Sessions are established via asymmetric cryptography (Curve25519) with users' public keys.

Once a session is establish, symmetric cryptography (AES-CBC-256) is used along with hash authentication (HMAC-SHA256) to encrypt/decrypt and authenticate messages.

More cryptography in WhatsApp

Other use of end-to-end cryptography in WhatsApp:

- images
- voice calls
- group messaging

An additional encrypted layer for the communication between WhatsApp clients and WhatsApp servers.

WhatsApp's security

This depends strongly on the correctness of the public-key component of the identity key pair that is registered by each client with the WhatsApp server.

In order to be sure that PK_B^{Id} received from the server actually comes from Bob, Alice can either request from Bob a QR code containing PK_B^{Id} or compare with Bob a 60-digit check number computed using SHA-512 from both PK_A^{Id} and PK_B^{Id}.

Possible issues with WhatsApp and other messagers

1) Anyone who controls WhatsApp's servers could effortlessly insert new people into an otherwise private group, even without the permission of the administrator who ostensibly controls access to that conversation.

Paul Rösler, Christian Mainka, Jörg Schwenk, *More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema*, Proceedings of 3rd IEEE European Symposium on Security and Privacy (EuroS&P 2018), published online January 15th, 2018.

Possible issues with WhatsApp and other messengers

2) Collection of metadata

Using end-to-end encryption does not prevent messaging services from collecting metadata (e.g. whom you called at what time, how frequently, etc.). WhatsApp's FAQ states that its app has access to all the phone numbers in your address book, and that it collects a myriad of information about you. For example:

"Please note that WhatsApp regularly looks at the phone numbers in your phone's address book and then checks to see which of those numbers are verified in WhatsApp. Any WhatsApp users from your address book will appear as contacts you can message in WhatsApp. During this entire process, phone numbers are sent to WhatsApp for lookup, securely, over an encrypted connection. In order to know who you're chatting with, the app displays the names from your address book."

3) Collection of messages when using clouding services

E.g. iCloud when you backup the iphone.

Test questions

Question 31

Take a messaging service other than WhatsApp and try to determine whether the service:

(a) encrypts messages;

(b) allows the service provider access to the content of messages;

(c) provides perfect forward secrecy.

Question 32

Find out how WhatsApp uses cryptography to:

(a) protect a large file attachment such as a photo;

(b) secure a message sent from one user to a group of other users.