Meow messaging protocol

Author meow@redroom.link

December 12, 2023

Abstract

The Meow protocol is a privacy driven instant messaging protocol. That protocol might be used for creating secure and distributed chat services or allowing machine to machine communication. This document describes the services provided by the protocol.

> *"Nous ne vivrons pas d'utopie collective, nous arrivons trop tard, le grand marché est déjà là. Nous devons élaborer des stratégies de survie et de contamination, par la prolifération d'utopies privées, cryptées, qui se substitueront à l'ancien ordre social. Tout ce que je sais, c'est que nous vivons dans un monde dont on ne s'évade pas"*
> Maurice G. Dantec for NOII (1997)

1 Services

1.1 Unregulated identities

The only requirement to get a valid Meow identity is to generate a user key pair. No phone number or email check will be performed, unlike main instant messaging protocols, there is no central administration.

1.2 Fine grained privacy control

1.2.1 Trustable server based communication

Like most widely available messaging softwares, (Whatsapp, Signal, Viber, Telegram...), Meow provides a simple server based messaging. The main difference is that Meow allows you to explicitly choose which server you want to use. The server code being open source, we strongly encourage you to run your own server at home or in your company. The server requires very few ressources and will run on any low cost single board computer.

1.2.2 Anonymized message transfer

Meow also provides an anonymizing transfer service very similar to the Tor Onion protocol, we call it the Matriochka protocol. Any server can be used for building the transfer chain. Some of them might be marked as trusted. Random delays and random payload padding might be set for each forwarding step, making the overall message tracking much more difficult, even for organizations having capabilities of global network surveillance. It is strongly advised to use trusted servers as your first node and message server (the one that holds your incoming messages).

1.2.3 Presence protocol for direct messaging

A presence service associating your conversation keys to your IP address for direct peer to peer connection is also provided. The presence protocol is simply activated by setting a flag in the message poll requests. If that flag is set, your encrypted IP will be published on the server, allowing your only your peer(s) to decrypt it and directly communicate with your terminal.

1.2.4 Peer based privacy settings

You might define specific communication privacy preferences for each of your contacts:

- simple server based communication allowed for Sarah,
- preferred direct communication with Julian, fallback to my own server,
- required matriochka protocol for Edward, first node is one of my trusted servers, my message node is my own server, randomly switch from trusted server lists for others.
- ...

1.2.5 Resistance to device requisition / forensic

All your contact information and discussion are encrypted on the device and password protected. Password shall be asked on application startup and allows your identity file and contact decrytion. That password is not recoverable, so you can't forget it, or you'll loose your whole configuration and identity. Real security implies some constraints. You might configure the app to save your password, but that is a security flaw. In many authoritarian countries, you are required by law to provide your device passwords to authorities. In a Meow device, you might set a specific password for some contacts. Those contacts won't be visible when entering your main identity password. You'll have to type their specific password in order to make them visible. The Meow application will by default create a random set of fake hidden contacts and conversations. Even in case of device storage analysis, authorities won't be able to differentiate a real hidden contact from an normal fake generated one. It could be argued that this feature puts every user at risk, because authorities might think you're hiding something, even if you're not. As every Meow user has the same constraint, users are not responsible for that. Moreover solidarity is also a requirement for real security.

1.3 Multiple devices support

Meow allows you to be connected from multiple devices and offers chat synchronization capability. A device might be revoqued anytime from any other one. Proof of your identity (password or other) shall be provided in order to grant device revocation.

1.4 Adding contacts

If you want to add a new contact, keys will be generated, then a contact card will be created. That contact card might be sent by any trustable communication means, or preferably from hand to hand, as a file on a flash disk or a QR code. In return your contact will provide a similar contact card as an answer to your invitation.

1.5 Contacts forwarding

By using the Meow protocol a user won't be able to forward your contact information without your consent. Each user knows you as a different identity, thus forwarding a known identity to another user is meaningless. Any message to that identity signed by another user than you would be discarded.

1.6 Group conversation

A very basic group messaging service is available. It allows to exchange group information between users. After that, a message to a group will send a copy of the message to each member.

1.7 Emergency broadcast

A local (server based) emergency broadcast service will be provided. It will provide the ability to send/receive broadcast messages to all users connected to the current server.

1.8 Public networks shortage resilience

Meow may run without Internet connection, either on an isolated wifi access point, or on a meshed network of wifi routers or even via serial IOT transport layers (LoRa,...)

1.9 User directory service

This service allows restoring a lost functionality of Internet historic chat services (like ICQ). You could simply set a "Free for chat" status that would allow other people to contact you, either randomly or based on a short description that you might provide. Why providing that service while the internet is suffocating due

to the abundance of social networks ?
Well, that option offers a few advantages :

- you are still an anonymous user chatting with other anonymous users;
- no social network algorithm will select people that think/behave/vote/eat... just like you. Diversity makes a better world;
- a smaller community of users, skilled enough to operate a MEOW chat app... that might provide a first filter; It's a bit like in the early ages, when people had to be able to start a win98 computer, connect it to internet, then download and install ICQ... If you lost some time in social networks today, and experienced ICQ in the 2000's, you'll understand what we'd like to revive.

2 Identities and keys

2.1 User identity

Each MEOW user has a unique identity. That identity is strictly private, only used to manage your own data (local encryption, devices, ...) Let's call that one the User Key Pair (Ukp)

2.2 Contact identity

Each of your contacts will know you under a different identity, we'll call that one the Contact Key Pair (Ckp) That contact Key Pair will not change once it's agreed between both peers: an initial key will be exchanged as part of the peer invitation process. As other people might have seen your key, this means that :

- none of your contacts will be able to forward your id to another person without your consent;
- any message to that Ckp, not signed by its associated user, will be discarded.

2.3 Conversation encryption

Each conversation with one of your contacts will be encrypted using an encryption keypair (Ekp) allowing cyphering your conversation. The Ekp might be changed anytime by its owner and the new public key will be sent along the last message.

2.4 Conversation lookup

A contact conversation Lookup Key Pair(Lkp) is also associated with your conversation. The Lkp public key is used to identify your conversation on a server. The private key allows you to sign your request and prove the server that you are the legitimate recipient for a message. This Lkp can be changed anytime by its owner and the new public key will be sent along the last message. The Lkp and the Ekp are only changed once the change has been acknowledged by your contact.

2.5 Server identity

Each server has a Server key (Skp). That key allows you to cypher the messages that you're sending to the server.

2.6 Device identity

Each device is identified by a device key (Dkp) that allows you to perform secured exchanges between your devices for synchronization/revocation purposes. Communication between devices is achieved using the same principle as the user to user communication. A device might be considered as any another user. The messages content is based on a synchronization protocol.

3 Contact management

3.1 Adding a contact

Rendez-vous card, containing :

- Your public key for that contact;
- An initial conversation public key for getting encrypted messages from that contact;
- An initial conversation uuid that you'll use to lookup for incoming messages on the servers;
- A list of your preferred message servers;
- A signature to prevent transmission of tampered data.

3.2 Sharing a contact

If a user wants to forward one of his contacts to you, it will be handled as a double request:

1. I'm receiving a contact name, without any key
2.

4 Messaging

4.1 User messages

TODO

4.2 Server stored message

TODO

4.3 Matriochka message packing

TODO

4.4 Synchronization messages

TODO

5 Server Features

5.1 Server catalog

Each server will cache a list of all the servers that it is aware of. This server list will be shared between servers in a lazy exchange mode.

5.2 Antispam

5.3 Self defense

The servers do integrate self defense mechanisms. Any threat to the Meow network by any computer, computer group or organization, might result in a distributed response from volunteering Meow servers and clients. An information about threat, desired defense action and request for assitance, might be submitted by any server or group of servers. Server owners and client users might accept or refuse to participate to the response action.

TODO : Request and actions definition consensus mechanism

6 Backup

7 Recovery

8 Very secure devices

You don't trust your phone ? We're planning to provide very secured minimal devices dedicated to very sensitive Meow communication.

9 Roadmap

9.1 Nations

Beyond the scope of user directories, we plan to implement the concept of virtual Nations. Nation will allow people to regroup around common political funding values. They're not exclusive, you might be a citizen of several virtual nations.

Today still, most people don't really choose the nation they live in. You just have to live with the goverment decisions. In the best scenario that government was elected, and might represent at most 25% of the population. In most case, they will vote laws to satisfy the powerful people who supported their election, and the most powerful lobbies.

Meow Nations aim to be the next lobbying power to influence real life politics, "the poor man's lobby".

Virtual nation in that perspective will be probably quickly flagged as terrorist nation by the old world media, but well, one man's terrorist is another man's freedom fighter. If requiring more democracy, using the same technique that is preventing it from happening, has to qualified that way, so be it.