End-to-End Encryption

Table of Contents

1. What is end-to-end encryption?
2. Benefits
3. Limitations
4. Popular protocols
5. Innovations
6. Application demo

What is end-to-end encryption?

- It is a communication channel which in which the messages can be read only by the intended recipients
- It is based on public key cryptography and the sender uses the public key of the receiver and encrypted the message
- Message encryption is done at the endpoint, so no third party can read their contents unless they have the private key to decrypt them

Benefits

- Message contents remain private
- Users do not need to rely on third parties
- Protection against data breaches
- Compliance with privacy and security regulations

Limitations

- Metadata can be collected
- Endpoint security
- Backdoors
- Man-in-the-middle attacks
- Spam and abuse are harder to filter out

Popular protocols

The following protocols have gained popularity in the recent years either through their implementation in the most used applications, or security promises and innovations in the field.

- Signal: Signal, Whatsapp, Facebook Messenger (secret chats feature), Wire, Skype (secret conversations)
- MTProto: Telegram
- Signcryption: iMessage
- Letter Sealing: LINE
- Threema

Innovations

- Double ratchet algorithm (Signal)
- Sealed sender (Signal)
- Forward secrecy (OTR)
- MLS - Messaging Layer Security

Application demo

Features presented:

- Login and Register
- Add conversation
    - Private chat - encrypted and unencrypted
    - Group chat - encrypted and unencrypted
- Send messages and attachments
- Third party view - encrypted and unencrypted chats
- Logout