# Poll

**Order these messengers from most secure to least secure**

Whatsapp

Facebook Messenger

VK

Telegram

Signal

iMessage

# Telegram’s famed security

## Is it me or is Tg creepy is fcuk?

I_van https://unmb.pw  tg: @schpongle

# Disclaimer

- I’m not a ~~lawyer~~ security expert
- Follow links in this talk.
- Do your own research
- Prove me wrong!
- I’m biased, as vans are natural telega’s rivals

# Plan

- What people expect from Telegram?
- Tg’s claims and promo materials
- Actual security features
- Competition
- Conclusions

**I_van https://unmb.pw  tg: @schpongle**

# Poll results

# telegram.org

## Why Telegram?

### Simple

**Telegram** is so simple you already know how to use it.

### Private

**Telegram** messages are heavily encrypted and can self-destruct.

### Synced

**Telegram** lets you access your chats from multiple devices.


### Fast

**Telegram** delivers messages faster than any other application.

### Powerful

**Telegram** has no limits on the size of your media and chats.

### Open

**Telegram** has an open API and source code free for everyone.

### Secure

**Telegram** keeps your messages safe from hacker attacks.

### Social

**Telegram** groups can hold up to 200,000 members.

### Expressive

**Telegram** lets you completely customize your messenger.

# telegram.org/faq

- "Telegram is a messaging app with a focus on speed and security"
- "Telegram is more secure than mass market messengers like WhatsApp and Line"
- "Thanks to Telegram's multi-data center infrastructure and encryption, it is faster and way more secure"
- "Q: Do I need to trust Telegram for this to be secure?
  A: When it comes to secret chats, you don’t"

- "Q: Why not just make all chats 'secret'?"
  -- More on that later

- "Q: Why should I trust you?
  A: Telegram is open, anyone can check our source code, protocol and API"

# What I’m looking at

- Given a choice of *something* vs security, do they pick security?
- How easy it is to use securely?
- Independent security audit?
- Bug bounty?
- Open source?

**I_van https://unmb.pw  tg: @schpongle**

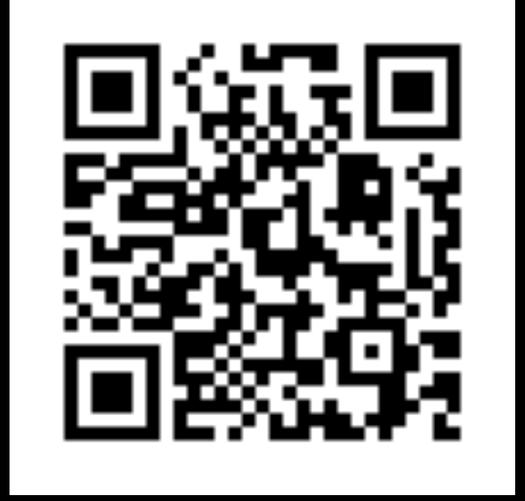
# Crypto protocol

# Crypto protocol

- Uses AES in IGE mode, which literally no one else uses
- Custom key derivation function
- Whatever

# Crypto protocol

https://news.ycombinator.com/item?id=6915741



> Just at a glance, the use of modes like Infinite Garble Extension (a failed mode for Kerberos) is troubling, they made up their own KDF (with no proof), and they make what appear to be some amateur mistakes with how they use RSA.

> IGE is an extremely weird, and, at this point I'll venture: bad choice for a 2013-2014 cryptosystem.

Crypto protocol
HN discussion



Crypto protocol
HN discussion

# Cringe protocol

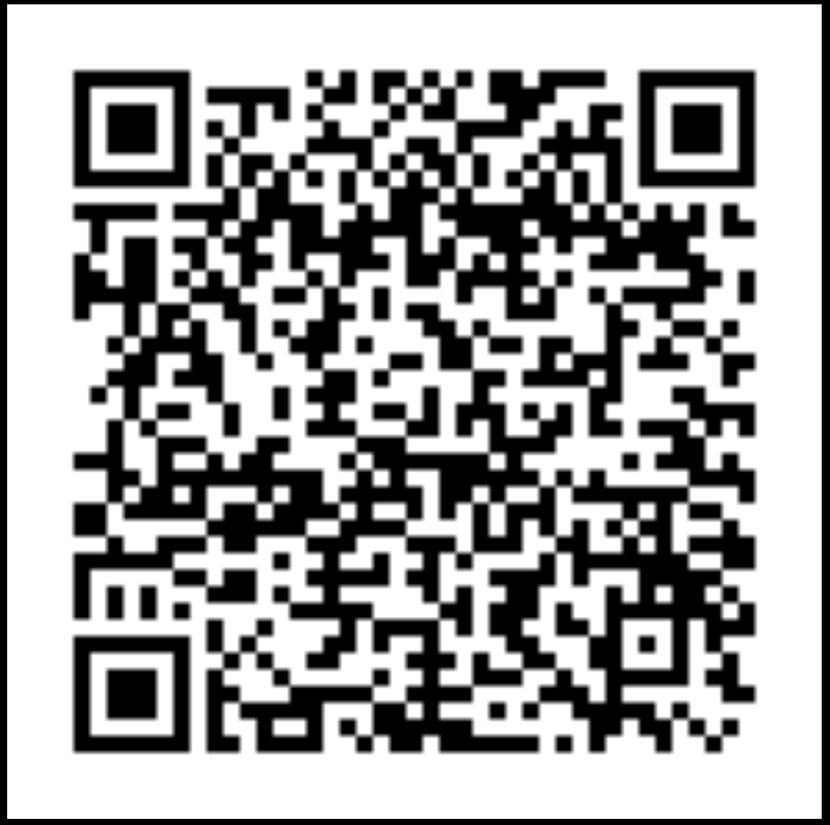
Telegram:
As for KDF, going for slower provable algorithms used for each incoming\outgoing packet may be a preferred solution for projects aimed at the relatively small security crowd. But we don't really compete in this area, our competition is WhatsApp and other mass market messengers.

Moxie:
That's interesting, because the thing you've made up is actually slower than a provably secure KDF.

# “The Most Backdoor-Looking Bug I’ve Ever Seen”

https://buttondown.email/cryptography-dispatches/archive/cryptography-dispatches-the-most-backdoor-looking/

This bug allowed Telegram to intercept all Secret Chat content because of their extremely weird protocol decision.

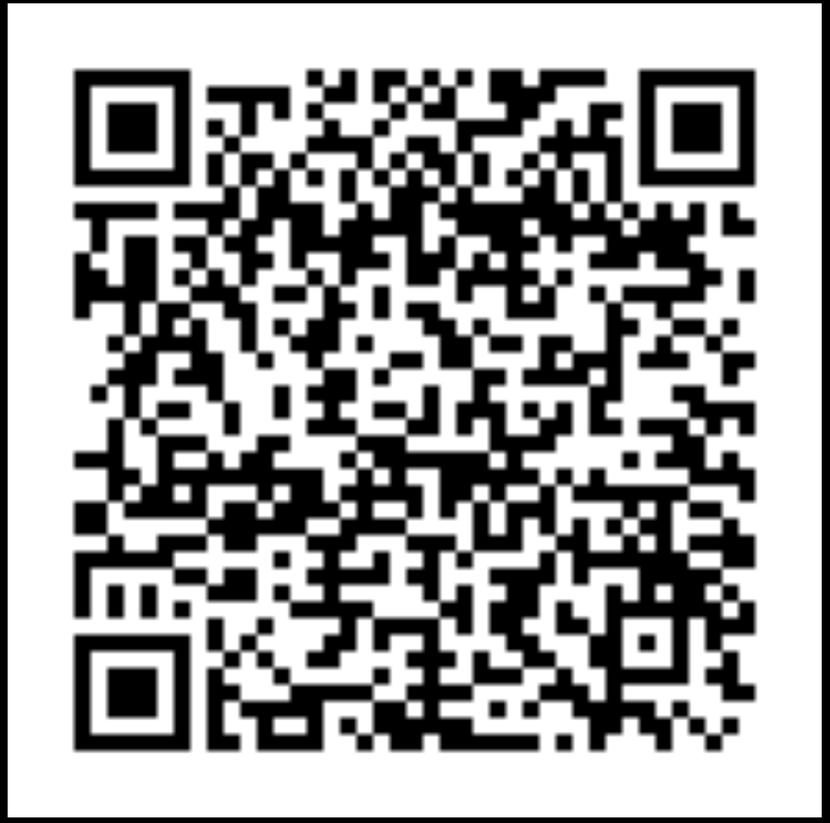


# “The Most Backdoor-Looking Bug I’ve Ever Seen”

TLDR:

Tg client used "randomness" provided by the server

WTF?



# Cringe protocol

MTProto— is not IND-CCA secure — theoretical attack
Fixed in MTProto 2.0

https://eprint.iacr.org/2015/1177.pdf

# Crypto protocol

Alleged performance > Security

# End to end encryption

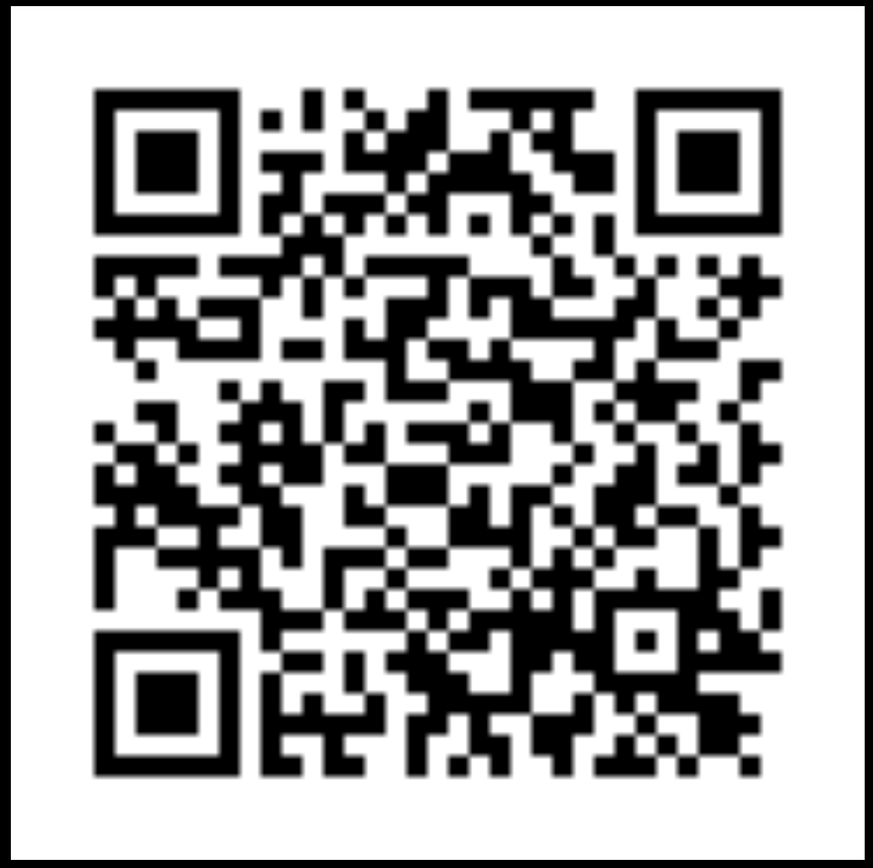
# E2EE

Disabled by default

Why: https://telegram.org/faq#q-why-not-just-make-all-chats-39secret-39

In short:

- To store backups
- Get chat history on new device



E2EE

# Usability > Security

# E2EE - Backups

"reliable backups are an essential feature for any mass-market messenger.
To solve this problem, some applications (like Whatsapp and Viber) allow decryptable backups that put their users' privacy at risk – even if they do not enable backups themselves."

**I_van https://unmb.pw tg: @schpongle**

# E2EE - Backups

So what Telegram is saying is:

Unencrypted messages on Telegram servers
are somehow better than
Unencrypted messages on Apple or Google servers.

# E2EE - Backups

Whatsapp:
Turn off backups —> E2EE in all conversations with no plaintext anywhere except your phone

How do I get E2EE in all conversations in Telegram?

**I_van https://unmb.pw tg: @schpongle**

# E2EE - Backups

Whatsapp now has encrypted backups

I_van https://unmb.pw tg: @schpongle

# E2EE - Backups

Signal doesn’t use backups

I_van https://unmb.pw tg: @schpongle

# E2EE - Message history on new devices

Do you actually need it?

What if I value security more than history

I_van https://unmb.pw tg: @schpongle

# E2EE - Message history on new devices

Can I turn it off it Telegram?

No

I_van https://unmb.pw tg: @schpongle

# E2EE - Usability

Telegram:

- Desktop: Not supported at all
- 4 clicks to start a “Secret Chat”
- Multiple “Secret Chats” per user

(???)

**I_van https://unmb.pw  tg: @schpongle**

# E2EE - Usability

Whatsapp, Signal:

- Works on desktop
- Enabled by default (And is the only option!)

# E2EE - Usability

How do you check the keys?

Is it easy?

Have Tg ever advised you to do that?

**I_van https://unmb.pw  tg: @schpongle**

E2EE

# Alleged usability > Security

If you care about usability then why is it worse than any other E2EE messenger?

**I_van https://unmb.pw  tg: @schpongle**

# E2EE - Competition

E2EE:

Whatsapp (2 billion users)
iMessage (? million users)
Line (86 million users)
Signal (> 40 million)

Not E2EE:

Facebook (1 billion users)
Telegram (0.7 billion
WeChat (1.2 billion)

Most western apps are E2EE
Surely they’re usable enough

# Nitpick: “Secret Chat” naming

# Nitpick: “Secret Chat” naming

Definition of “secret” (adj) - Merriam Webster

a : kept from knowledge or view : hidden
b : marked by the habit of discretion : closemouthed
c : working with hidden aims or methods : undercover a secret agent
d : not acknowledged : unavowed a secret bride
e : conducted in secret a secret trial

# Nitpick: “Secret Chat” naming

It’s not “Secret”, it’s not more hidden from anyone than “Not Secret”

Better naming: “Secure Chat” vs “Insecure chat”

Would you like to use “Insecure Chat”?

**I_van https://unmb.pw  tg: @schpongle**

# Authentication

Auth

# SMS

Optional Pin

**Auth**

# Vulnerable to SIM Swap attacks

By default

# SIM Swap attack 1

1. Go to the carrier’s office
2. Tell them you’ve lost your SIM Card
3. Give them a fake passport of your victim
4. Get a SIM Card with your victim’s phone number

# SIM Swap attack 2

1. Work at the victim’s carrier
2. Give yourself a SIM Card with your victim’s phone number

# SIM Swap attack 3

1. Have a friend at the victims carrier
2. Ask them to give you a SIM card of your victim’s carrier

# SIM Swap attack 4?

1. Get an account at black market darknet website
2. Pay to get a SIM card of your victim’s phone number

I have no proof it’s possible, but I suspect it is

# SIM Swap attack 5

1. Be the government
2. Force the carrier to give you a SIM card with your victim’s phone number

# SIM Swap attack actual cases

- SIM swap attack on Jack Dorsey (Twitter CEO):

  https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

- On April 29 (2016), two Russian opposition activists reported that their Telegram messenger accounts had been hacked remotely. Georgy Alburov, a leading member of the Anti-Corruption Foundation, and Oleg Kozlovsky, the director of the Vision of Tomorrow Center in Moscow, believe unauthorized access to their accounts was obtained through tampering with the app's SMS login feature

  https://advox.globalvoices.org/2016/05/02/is-telegram-really-safe-for-activists-under-threat-these-two-russians-arent-so-sure/

- There are lots more

# SIM Swap attack on ACF / ФБК Telegram

# SIM Swap vulnerability of msgr apps

- Telegram - Vulnerable
- Whatsapp - Partially vulnerable
- Facebook - ? Haven’t checked but suspect it’s not
- Signal - Not vulnerable
- VK - Probably not, but haven’t checked

# Bug Bounty

# Bug Bounty

Yes

## Bug Bounty

# NDA

Researcher cannot tell anything to anyone at any time about the vulnerability they've found

# Bug Bounty

# NDA

"Консультант не должен ни в течение срока действия настоящего Соглашения, ни в любое другое время после его расторжения: 9.1.1. разглашать или передавать любую Конфиденциальную информацию любому лицу, компании, юридическому лицу или другой организации"

## Bug Bounty

# NDA

Which means Telegram doesn’t have to fix any bugs ever.

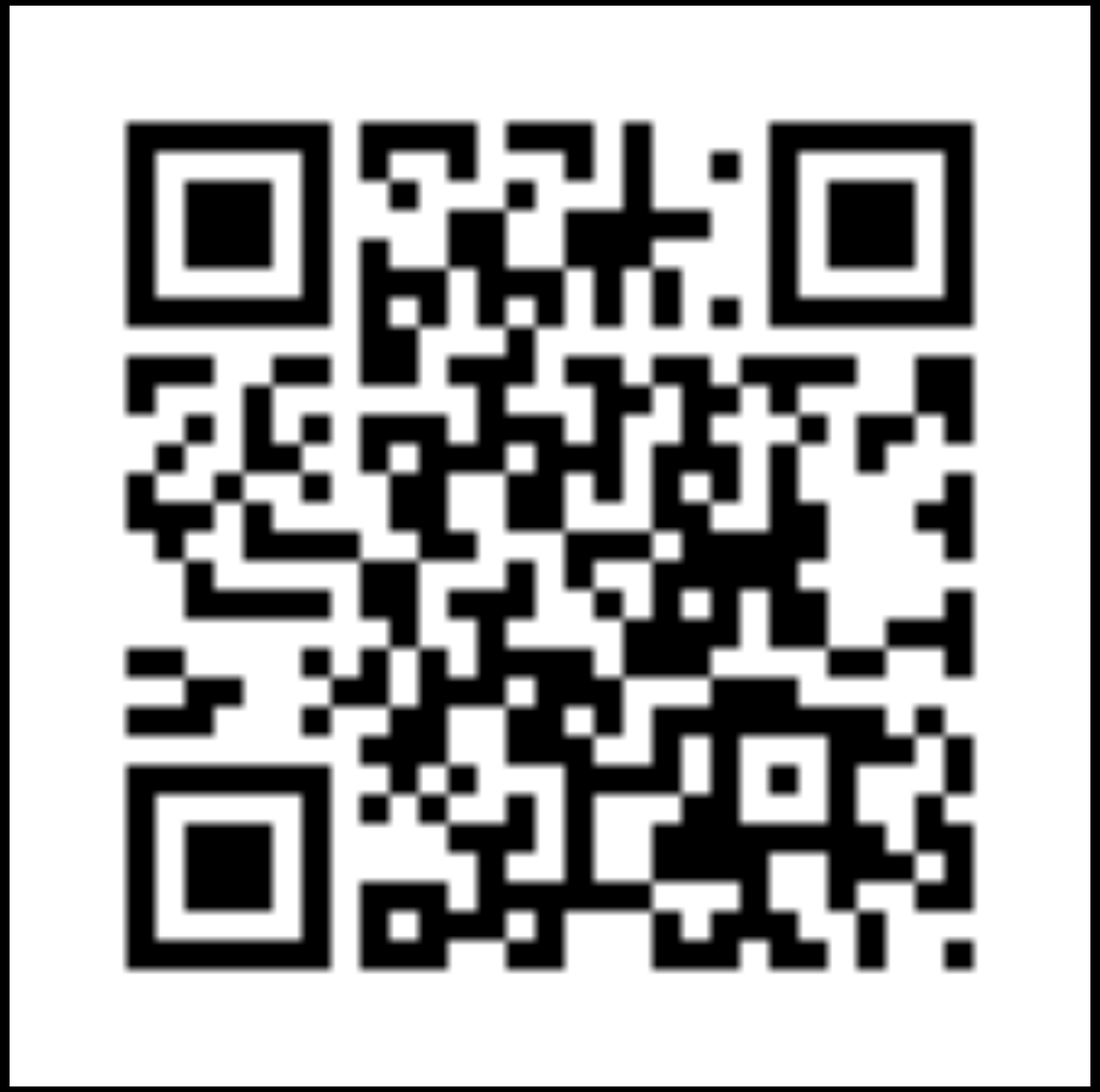
No deadline, no nothing

# Bug Bounty

Acutal researcher’s experience

https://habr.com/en/post/580582/

# Researcher’s bug bounty experience



# Bug Bounty

It’s basically the same as most other bug bounty programs

Most of them are shit

# Formal security audit

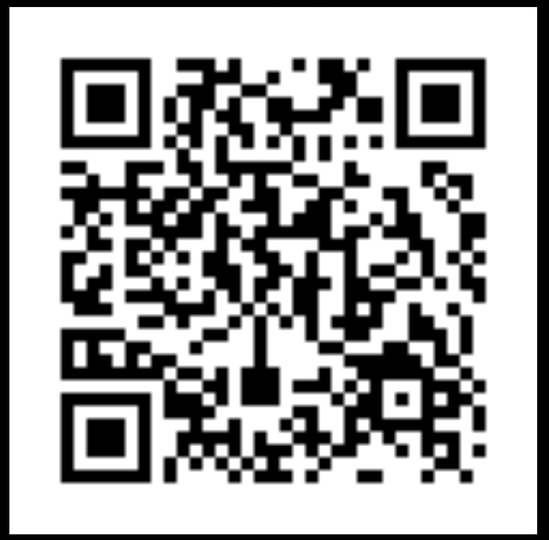
# Formal security audit

# Nope

# Formal security audit

> Мы не хотим платить журналистам и исследователям, чтобы они рассказывали о Telegram.
> Мы рассчитываем на вас — на миллионы наших пользователей. Если вам нравится Telegram, вы расскажете о нём своим друзьям

П.Дуров



https://telegra.ph/Pochemu-WhatsApp-nikogda-ne-budet-bezopasnym-05-16-7

“Crypto contest”

# “Crypto contest”

**The rules**

- Telegram sends a message to someone
- Publish encrypted traffic
- If you can decrypt it and read the message Tg pays you $200 000

Wat

# “Crypto contest”

## Is it common practice?

# No

“Crypto contest”

# Does it prove anything?

# No

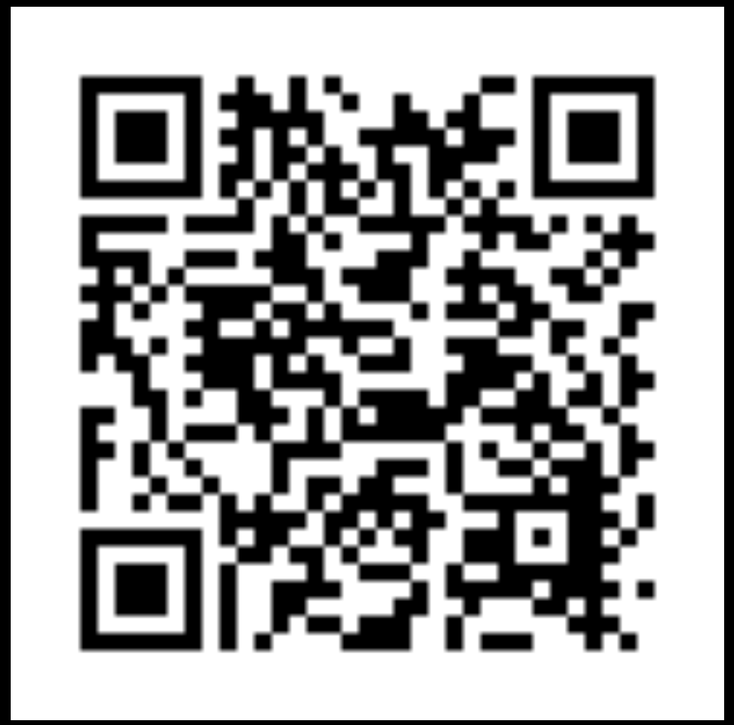
# “Crypto contest”

"If you want to show that a system is secure, give the adversary as much power as possible, and if they still can’t break it, the security is good"

# “Crypto contest”

# Why is it useless?

https://www.cryptofails.com/post/70546720222/telegrams-cryptanalysis-contest



You cannot modify traffic. The government can.

You don't know any of the plaintext. The government knows.

Participants don't have as much compute power as the government.

Because of that, even old and provably broken crypto will pass this contest.

# Open Source

# Open Source - story time

(optional)

# Open Source

Right now it is

Often releases source code months after binaries

# Telegram’s values

| Claimed | vs | Actual |
| --- | --- | --- |
| Performance | | Performance |
| Security | | Be perceived as secure |
| Usability | | Usability (?) |

# Comparison

**Whatsapp ( 3 / 5 )**

E2EE - Signal protocol
Partially vuln to SIM Swap
Closed Source
Bug Bounty - yes
Security audit - no

**Signal ( 4.5 / 5 )**

E2EE Signal protocol
Not vuln to SIM Swap
Open Source
Bug Bounty - no
Security audit - yes

**iMessage ( 3 / 5 )**

E2EE unknown proto
(can’t check keys?)
Not vuln to SIM Swap?
Closed Source
Bug Bounty - yes
Security audit - no

**VK ( -∞ / 5 )**

No E2EE - HTTPS
Not vuln to SIM Swap?
Closed Source
Bug Bounty - yes
Security audit - no

Operated by FSB

**Facebook ( 2 / 5 )**

No E2EE - HTTPS
Not vuln to SIM Swap?
Closed Source
Bug Bounty - yes
Security audit - no

**Telegram ( 1.5 / 5 )**

Weird protocol
E2EE only for 1 to 1 voice calls
( but can’t check keys )
Vuln to SIM Swap
Open? Source
Bug Bounty - yes
Security audit - no
Claims focus on security

## Security based on vibes

| Expectations | v s | Reality |
|---|---|---|
| Bad | Whatsapp | Good |
| Bad | Facebook msgr | Not good |
| Good | Telegram | Bad |
| Very Good | Signal | Very Good |
| FSB | VK | FSB |
| Good | iMessage | Good |

# Questions?

## Thank you Dilijan!

I_van https://unmb.pw  tg: @schpongle