RUHR-UNIVERSITÄT BOCHUM

RUB

Instant Messaging in Gruppen: Schwachstellen trotz sicherer Verschlüsselung

Tag der IT Sicherheit

2018-03-21

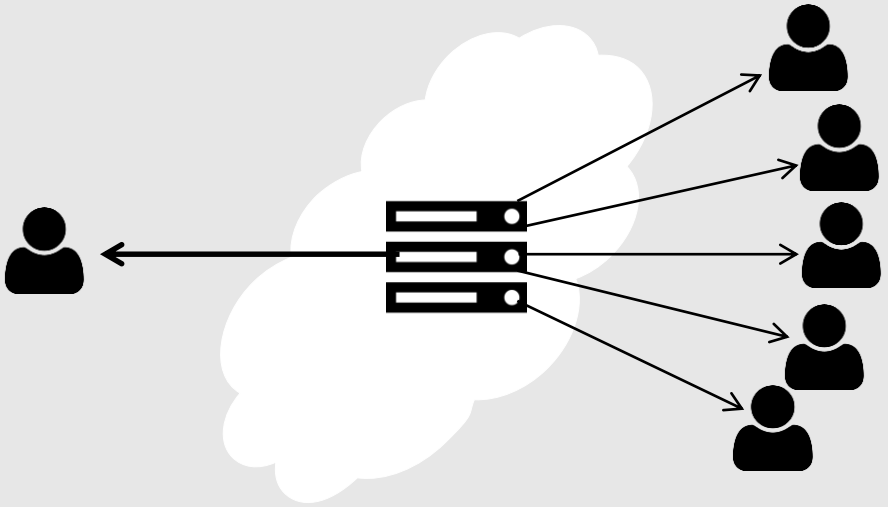
Horst Görtz Institute for IT Security
Chair for Network and Data Security
Paul Rösler, Christian Mainka, Jörg Schwenk

Secure Group Instant Messaging: End-to-End

- Dynamic group of users

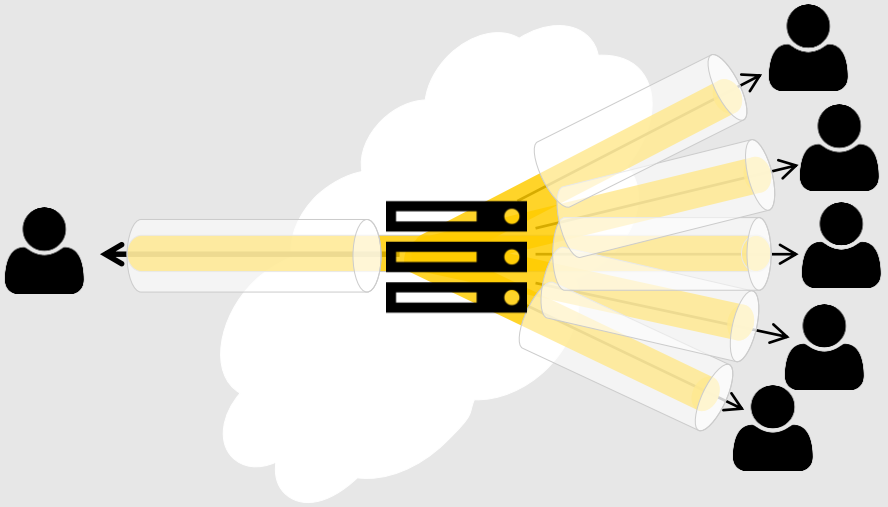
Secure Group Instant Messaging: End-to-End

- Dynamic group of users
- One central server (always online)



Secure Group Instant Messaging: End-to-End

- Dynamic group of users
- One central server (always online)
- End-to-end protection
  within protected transport layer
- Server potentially malicious



Secure Group Instant Messaging: End-to-End

- Dynamic group of users
- One central server (always online)
- End-to-end protection
  within protected transport layer
- Server potentially malicious

History of our Work

More is Less: How Group Chats Weaken the Security of Instant Messengers Signal, WhatsApp, and Threema

Paul Rösler, Christian Mainka, Jörg Schwenk
{firstname.lastname}@rub.de
Chair for Network and Data Security
Ruhr-University Bochum

July 24, 2017

Abstract

Secure Instant Messaging (SIM) is utilized in two variants: one-to-one communication and group communication. While the first variant has received much attention lately (Frosch et al., EuroS&P16; Cohn-Gordon et al., EuroS&P17; Kobeissi et al., EuroS&P17), little is known about the cryptographic mechanisms and security guarantees of SIM group communication.

In this paper, we investigate group communication security mechanisms of three main SIM applications: Signal, WhatsApp, and Threema. We first provide a comprehensive and realistic attacker model for analyzing group SIM protocols regarding security and reliability. We then describe and analyze the group protocols used in Signal, WhatsApp, and Threema. By applying our model, we reveal multiple weaknesses, and propose generic countermeasures to enhance the protocols regarding the required security and reliability goals. Our systematic analysis reveals that (1) the *communications' integrity* – represented by the integrity of all exchanged messages – and (2) the *groups' closeness* – represented by the members' ability of managing the group – are not end-to-end protected.

We additionally show that strong security properties, such as Future Secrecy which is a core part of the one-to-one communication in the Signal protocol, do not hold for its group communication.

History of our Work

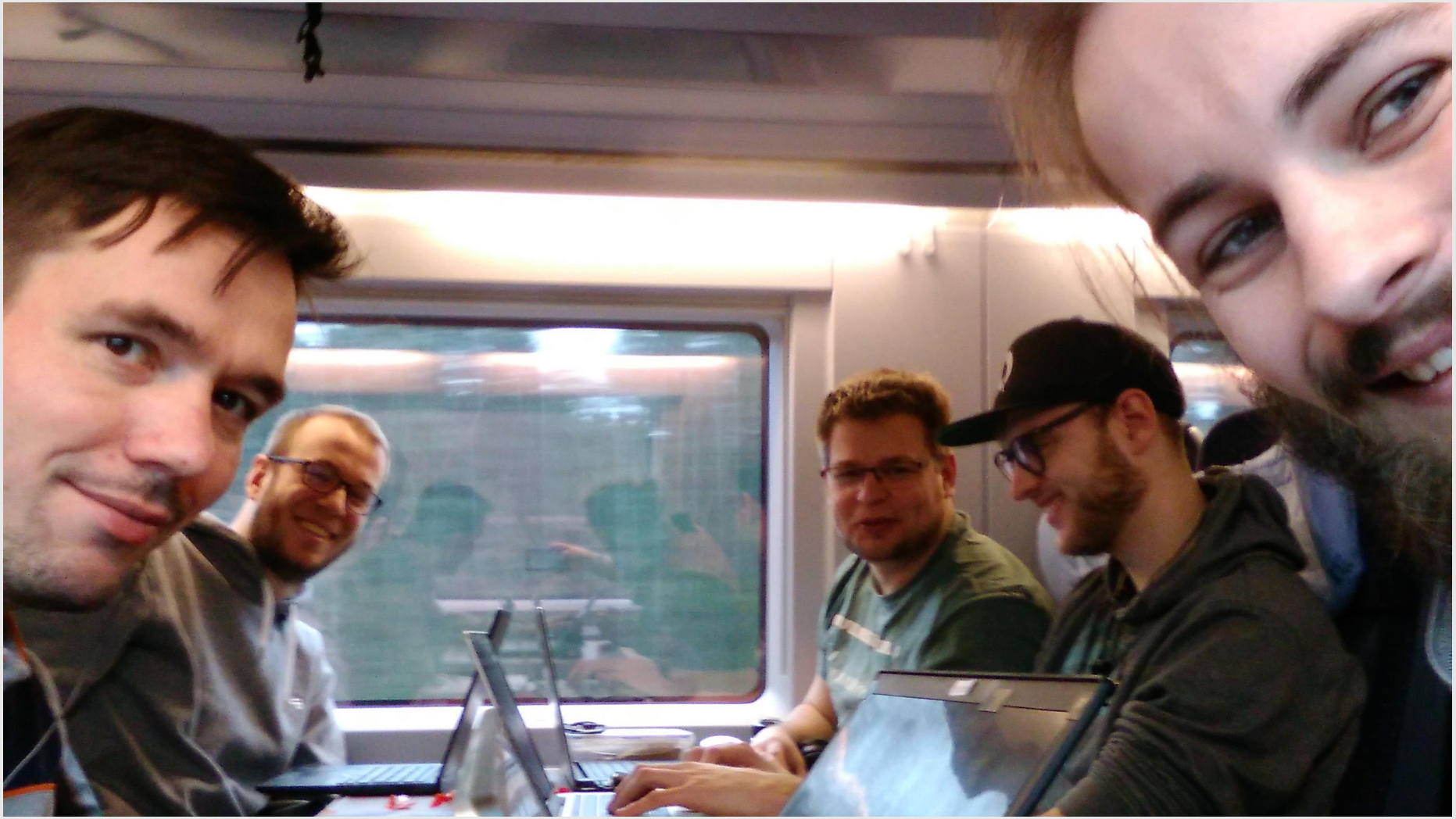
Real World Crypto 2018

Program

All going well with technology we plan to live stream the event, and keep a permanent record of talks at the RWC YouTube channel
https://www.youtube.com/c/RealWorldCrypto

Wednesday Jan. 10, 2018	
Session 5: Usability and privacy	session chair: Ian Goldberg
3:45pm	**Comparing the usability of cryptographic APIs** *Yasemin Acar (Leibniz University Hannover)*
4:15pm	**Is Certificate Transparency usable?** *Emily Stark (Google)*
4:45pm	**On the end-to-end security of group chats** *Paul Rösler (U. Bochum), Christian Mainka (U. Bochum), Jörg Schwenk (U. Bochum)*
5:10pm	**Privacy-preserving search of similar patients in genomic data** *Gilad Asharov (Cornell Tech), Shai Halevi (IBM), Yehuda Lindell (Bar-Ilan University), Tal Rabin (IBM)*
5:35pm	**End of day one**
5:45pm	**Reception**

History of our Work

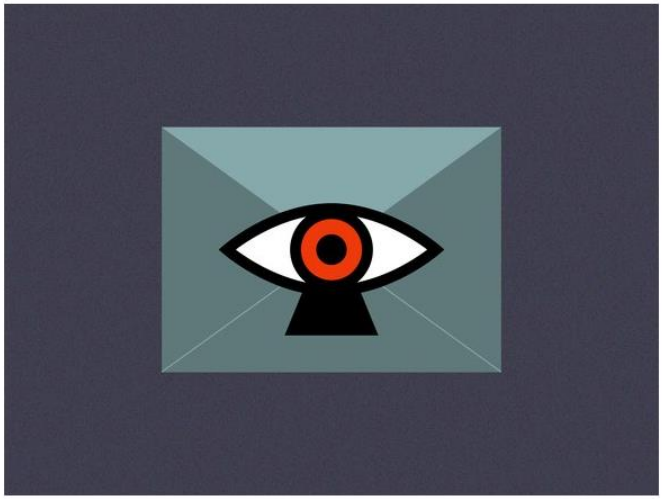


History of our Work

WIRED WhatsApp Security Flaws Could Allow Snoops to Slide Into Group Chats

ANDY GREENBERG SECURITY 01.10.18 07:00 AM

WHATSAPP SECURITY FLAWS COULD ALLOW SNOOPS TO SLIDE INTO GROUP CHATS



Millions of people trust WhatsApp's end-to-end encryption. But security researchers say a flaw could put some group chats at risk of infiltration. HOTLITTLEPOTATO

When WhatsApp added end-to-end encryption to every conversation for its billion users two years ago, the mobile messaging giant significantly raised the bar for the privacy of digital communications worldwide. But one of the tricky

Matthew Green in attacks, messaging January 10, 2018 1,984 Words

Attack of the Week: Group Messaging in WhatsApp and Signal

If you've read this blog before, you know that secure messaging is one of my favorite topics. However, recently I've been a bit disappointed. My sadness comes from the fact that lately these systems have been getting *too damned good*. That is, I was starting to believe that most of the interesting problems had finally been solved.

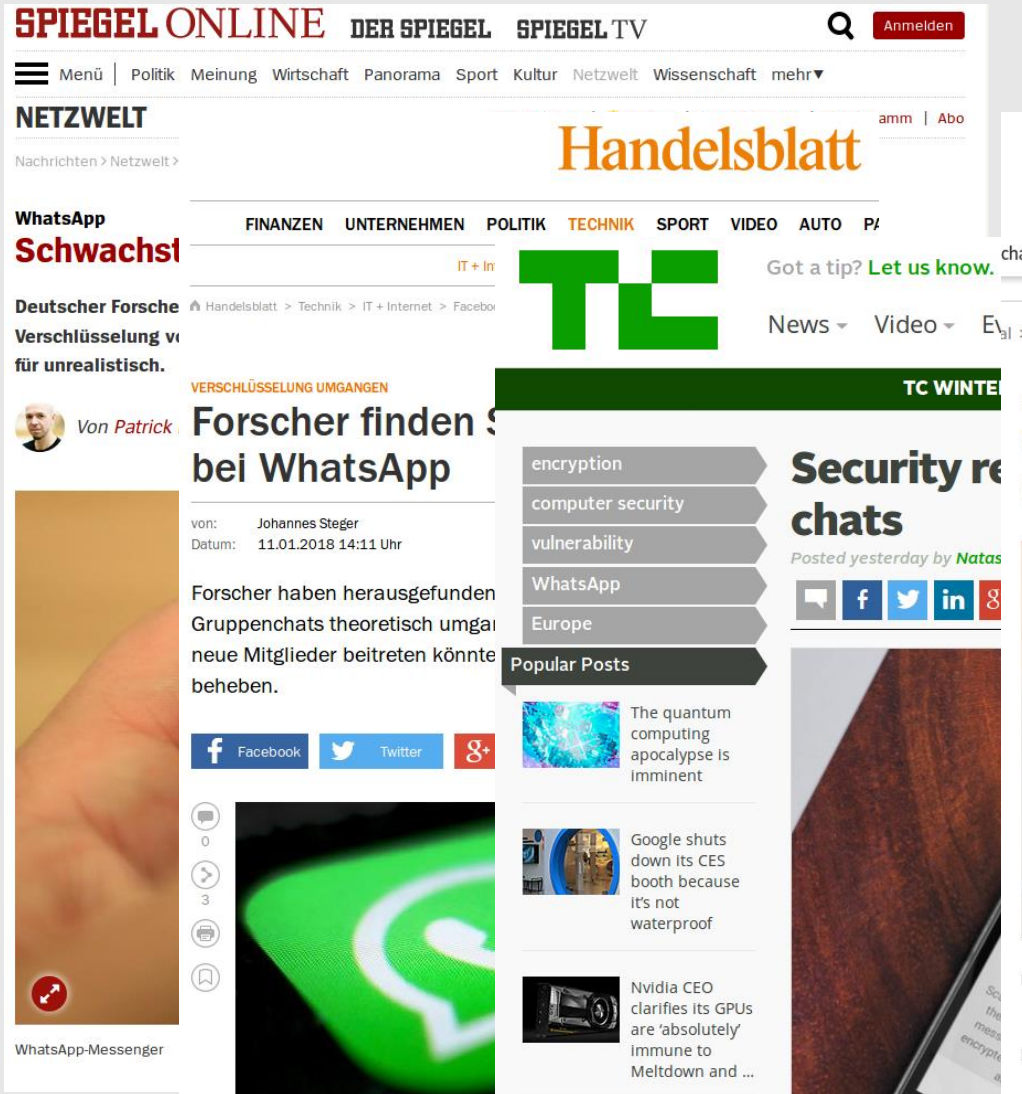
If nothing else, today's post helped disabuse me of that notion.

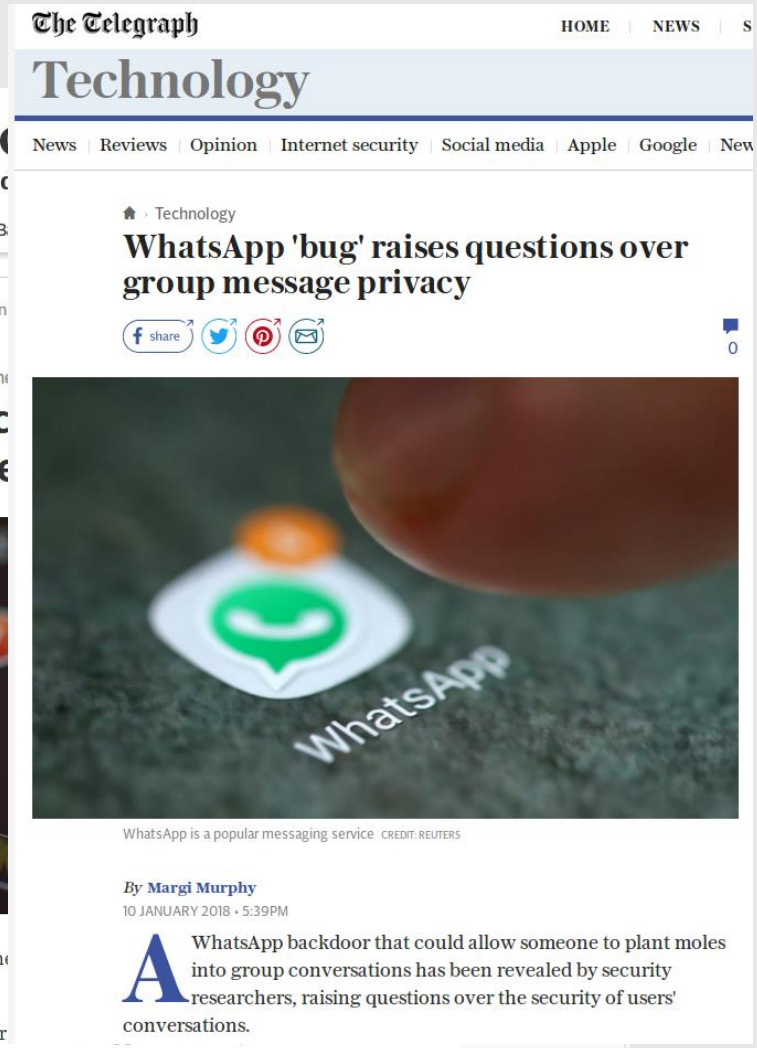
This result comes from a new paper by Rösler, Mainka and Schwenk from Ruhr-

Matthew Green

I'm a cryptographer and professor at Johns Hopkins University. I've designed and analyzed cryptographic systems used in wireless networks, payment systems and digital content protection platforms. In my research I look at the various ways cryptography can be used

History of our Work





History of our Work

THE Sun — THE SUN, A NEWS UK COMPANY

SPORT | TV & SHOWBIZ | NEWS | FABULOUS | MONEY

All Tech | Science | Phones & Gadgets | Gaming

WHO'S WATCHING? New Whats
bug could expose your group ch
messages to hackers – we reve
to stay safe

Researchers say WhatsApp users could vulnerable t
attack, as a new exploit reveals sneaky way of hack
private group chats

By Sean Keach
11th January 2018, 10:32 am | Updated: 11th January 2018, 2:32 pm

PRIVATE messages sent by WhatsApp users could be exposed thanks
software bug.

Researchers have revealed how hackers could break into the popular me
and read your conversations.

Bild — MENÜ

Resources | Industry Voice | SMB Spotlight

the INQUIRER

en Source | Hardware | Software | Security

Mail Online — Science & Tech

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Video | Travel | Fashion Finder

Latest Headlines | Science | Pictures | Discounts | Login

Massive WhatsApp security flaw lets ANYONE spy on conversations by secretly adding members to private group chats (but Facebook says it won't fix the problem)

- Security experts have found a way around WhatsApp's end-to-end encryption
- Hackers can insert people into WhatsApp groups without admin permission
- Facebook, which owns WhatsApp, said it does not intend to fix the issue
- It added that group chats 'remain protected' by the app's encryption

By HARRY PETTIT FOR MAILONLINE
PUBLISHED: 10:11 GMT, 11 January 2018 | UPDATED: 12:15 GMT, 11 January 2018

Share 160 shares 64 View comments

A huge WhatsApp design flaw that allows anyone to infiltrate private group chats has been uncovered by security researchers.

Despite the service's end-to-end encryption, experts say hackers can insert people

Site / Web — Enter your search — Search

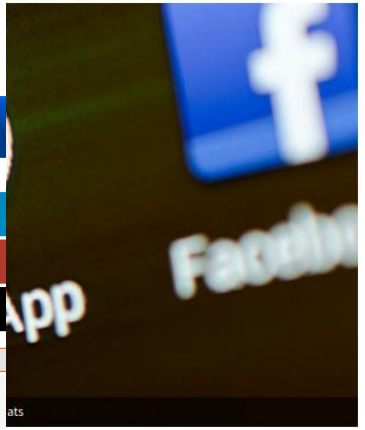
Like Daily Mail | Follow @dailymailtech | Follow Daily Mail | +1 Daily Mail | Download our iPhone app | Download our Android app

Today's headlines | Most Read

- Incredible NASA images show exposed 'undergound ice cliffs' on Mars in discovery that could provide...
- How clean is YOUR air? UK pollution hotspots are revealed using a new tool that lets you check toxic...
- Flashing fake eyelashes fitted with tiny LEDs could be the next high-tech beauty trend, but would you wear...
- General Motors says it will mass produce a self-driving car WITHOUT a steering wheel or pedals in 2019
- Little-known deep sea volcanic eruption that took place just 600 miles from New Zealand was the world's...
- Could dogs one day speak 'human'? Pet translator that converts growls and barks into English could be...

anyone easily
oup chats

shrugs off the issue



n a flaw that makes it possible for anyone to
in permission.

cryptographers from Ruhr University
findings at the 'Real World Crypto Security

History of our Work

Hacker News new | comments | show | ask | jobs | submit login

moxie 2 days ago | parent | favorite | on: WhatsApp Encryption Security Flaws Could Allow Sno...

Here's how WhatsApp group messaging works: membership is maintained by the server. Clients of a group retrieve membership from the server, and clients encrypt all messages they send e2e to all group members.

If someone hacks the WhatsApp server, they can obviously alter the group membership. If they add themselves to the group:

1. The attacker will not see any past messages to the group; those were e2e encrypted with keys the attacker doesn't have.

2. All group members will see that the attacker has joined. There is no way to suppress this message.

Given the alternatives, I think that's a pretty reasonable design decision, and I think this headline pretty substantially mischaracterizes the situation. I think it would be better if the server didn't have metadata visibility into group membership, but that's a largely unsolved problem, and it's unrelated to confidentiality of group messages.

In contrast Telegram does *no encryption at all* for group messages, even though it advertises itself as an encrypted messenger, and even though Telegram users think that group chats are somehow secure. An attacker who compromises the Telegram server can, undetected, recover every message that was sent in the *past* and receive all messages transmitted in the *future* without anyone receiving any notification at all.

There's no way to publish an academic paper about that, though, because there's no "attack" to describe, because there's no encryption to begin with. Without a paper there will be no talks at conferences, which means there will be no inflammatory headlines like this one.

To me, this article reads as a better example of the problems with the security industry and the way security research is done today, because I think the lesson to anyone watching is clear: don't build security into your products, because that makes you a target for researchers, even if you make the right decisions, and regardless of whether their research is practically important or not. It's much more effective to be Telegram just leave cryptography out of everything, except for your marketing.

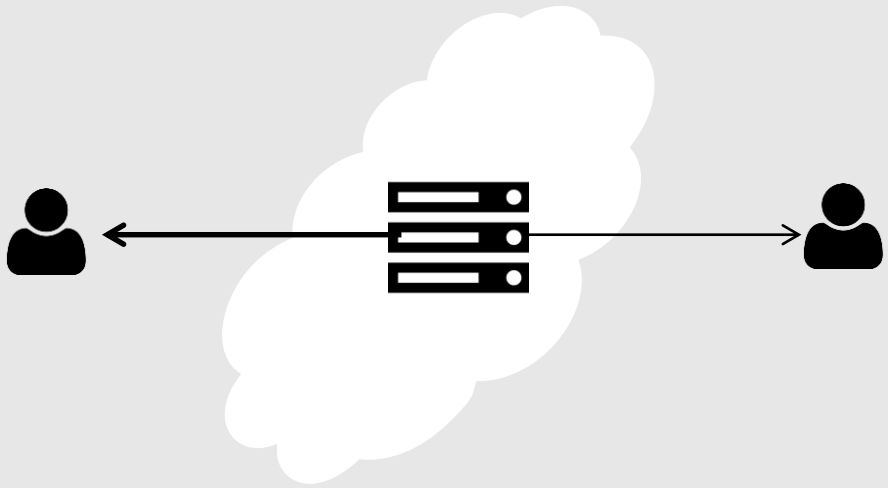
Agenda

- Security Model
  - End-to-End Encryption
- Protocol Overview and Weaknesses
  - Signal
  - WhatsApp
  - (Threema)
- Problems and Solutions
  - Traceable Delivery
  - Closeness

End-to-End Encryption

End-to-End Encryption

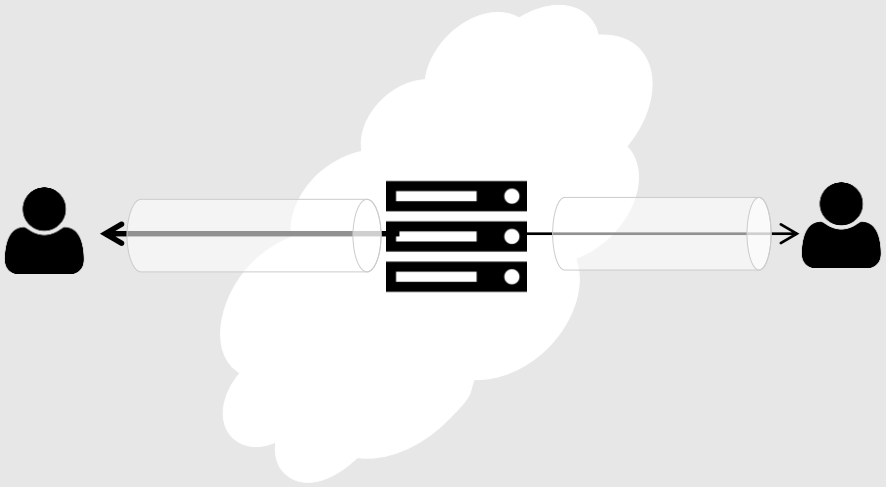
- Messages confidential
- Messages authentic



End-to-End Encryption

End-to-End Encryption

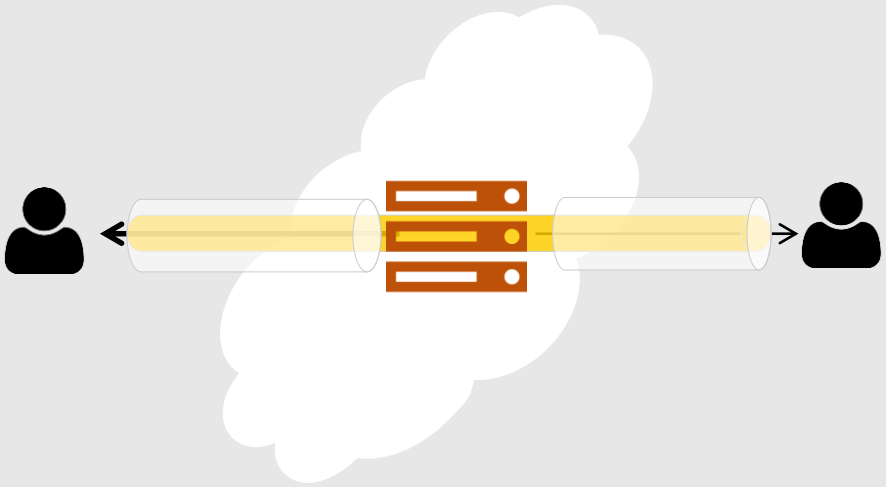
- Messages confidential
- Messages authentic



End-to-End Encryption

End-to-End Encryption

- Messages confidential
- Messages authentic



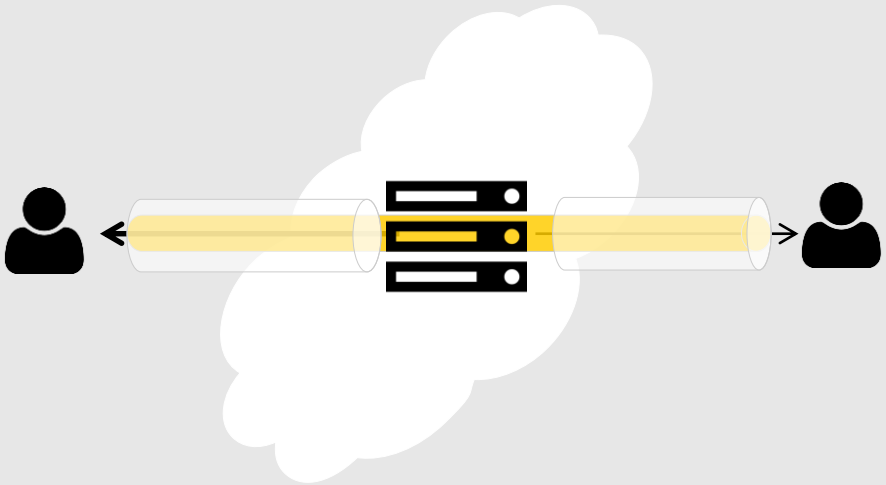
End-to-End Protection

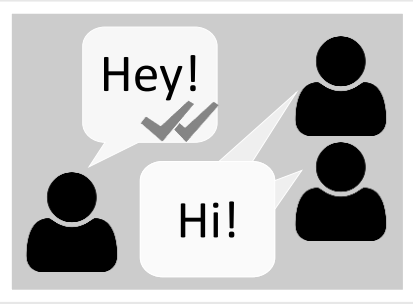
End-to-End Encryption

- Messages confidential
- Messages authentic

End-to-End Protection

- Message delivery reliable





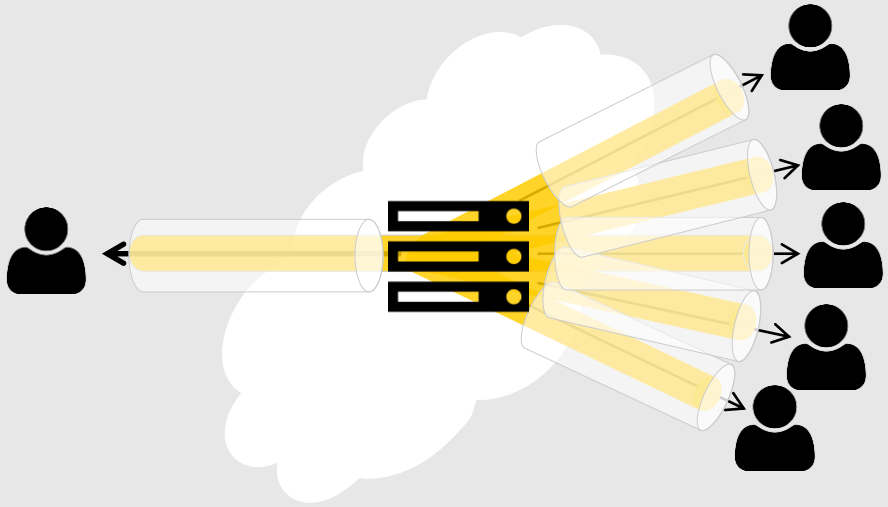
End-to-End Protection

End-to-End Encryption

- Messages confidential
- Messages authentic

End-to-End Protection

- Message delivery reliable



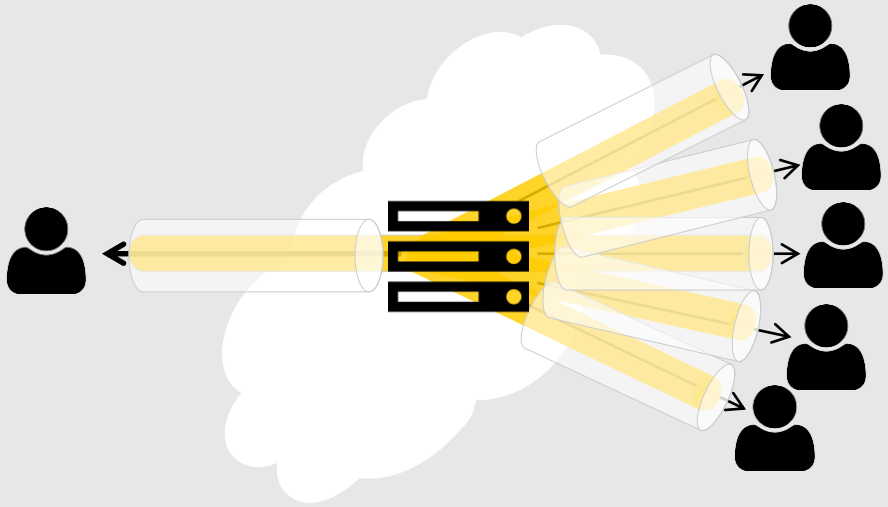
End-to-End Protection

End-to-End Encryption

- Messages confidential
- Messages authentic

End-to-End Protection

- Message delivery reliable
- Group management reliable



End-to-End Protection

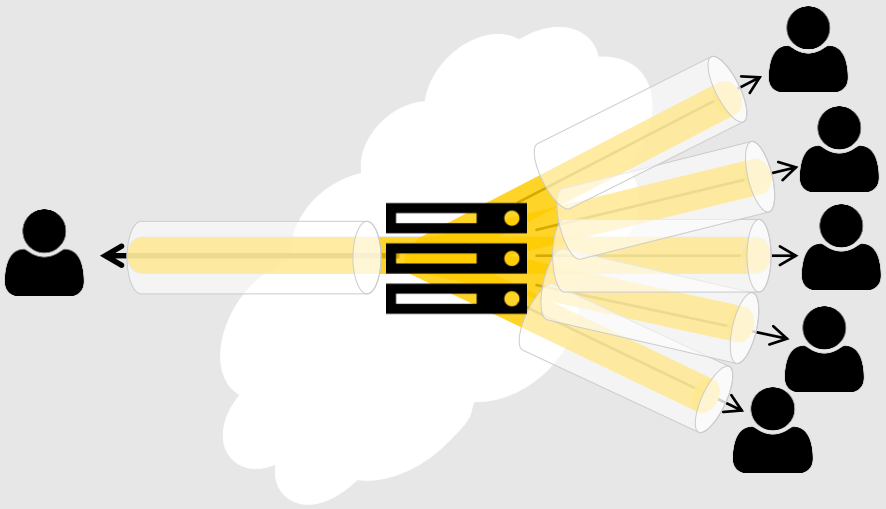
End-to-End Encryption

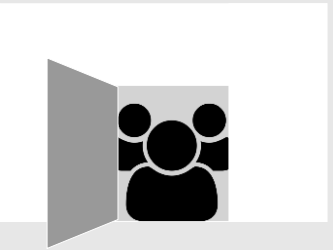
- Messages confidential
- Messages authentic

End-to-End Protection

- Message delivery reliable
- Group management reliable
- Group management “secure”

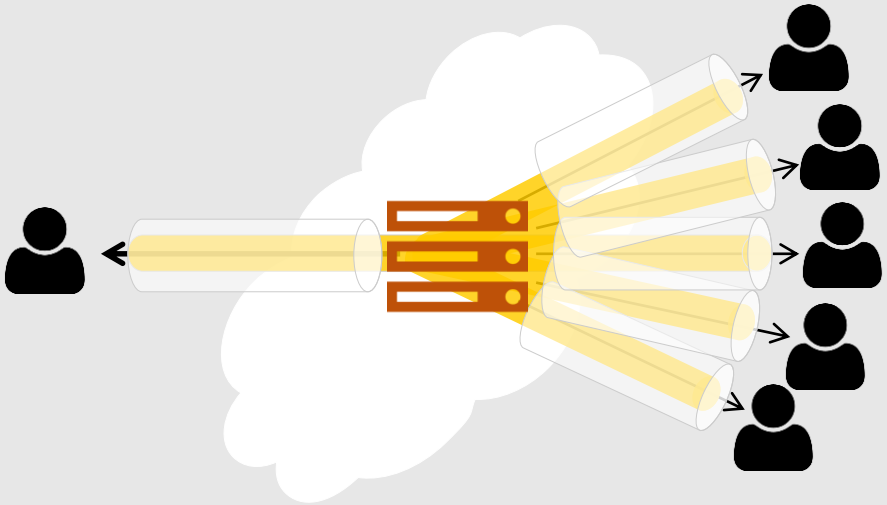
  → Members decide





Security Model: Malicious Server

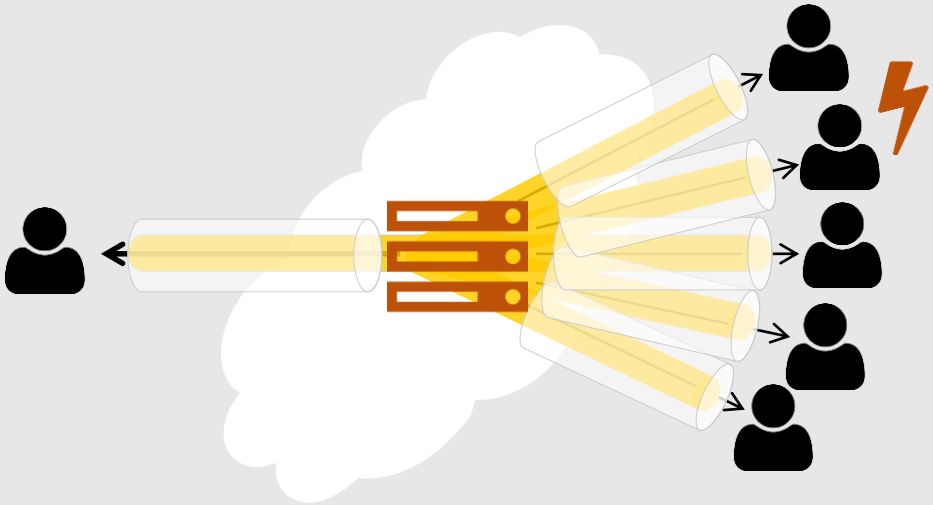
- Malicious Server
  - Can decrypt transport layer protection
  - E.g. IM provider, TLS certificate forger on network, ...



Attackable by		
		?

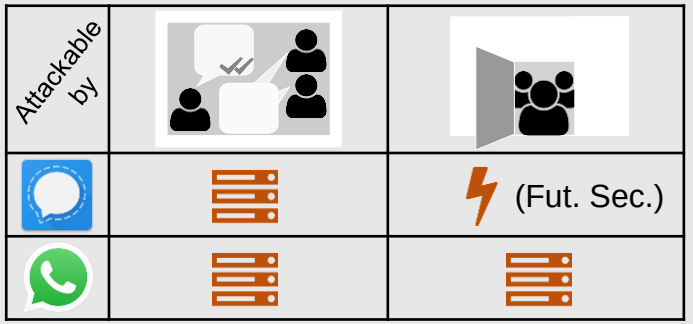
Security Model: Compromising Attacker

- Compromising Attacker
  - Access to members' secrets
  - E.g. access to device, cryptanalysis, …



- Advanced Goals:
  - Forward Secrecy

  - Future Secrecy
    (aka Post Compromise Security aka Backward Secrecy)



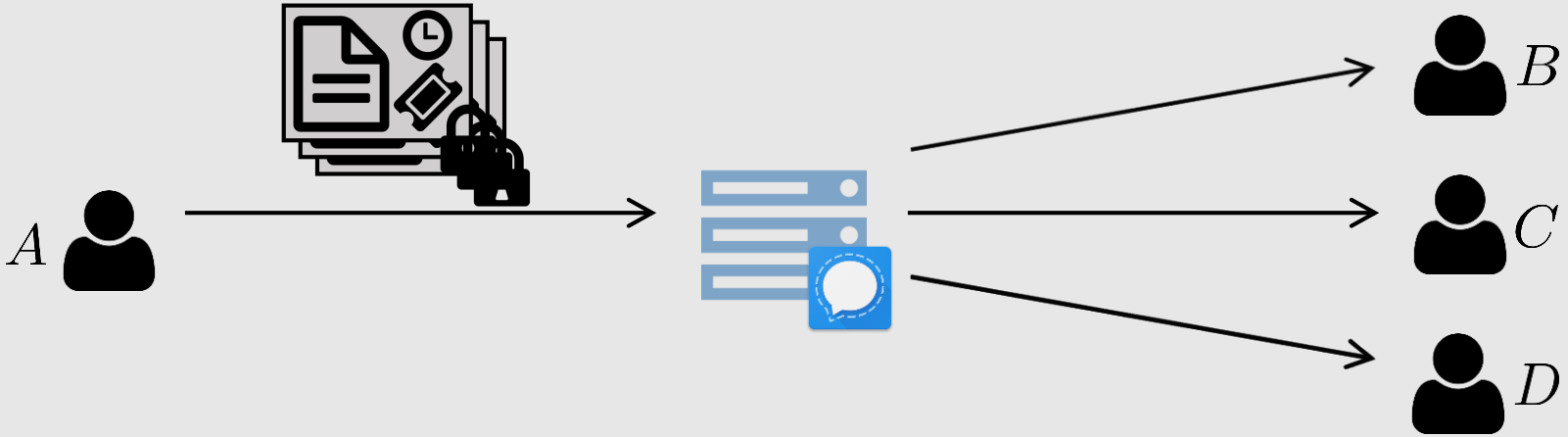
Protocol Overview: Signal

Protocol Overview: Signal

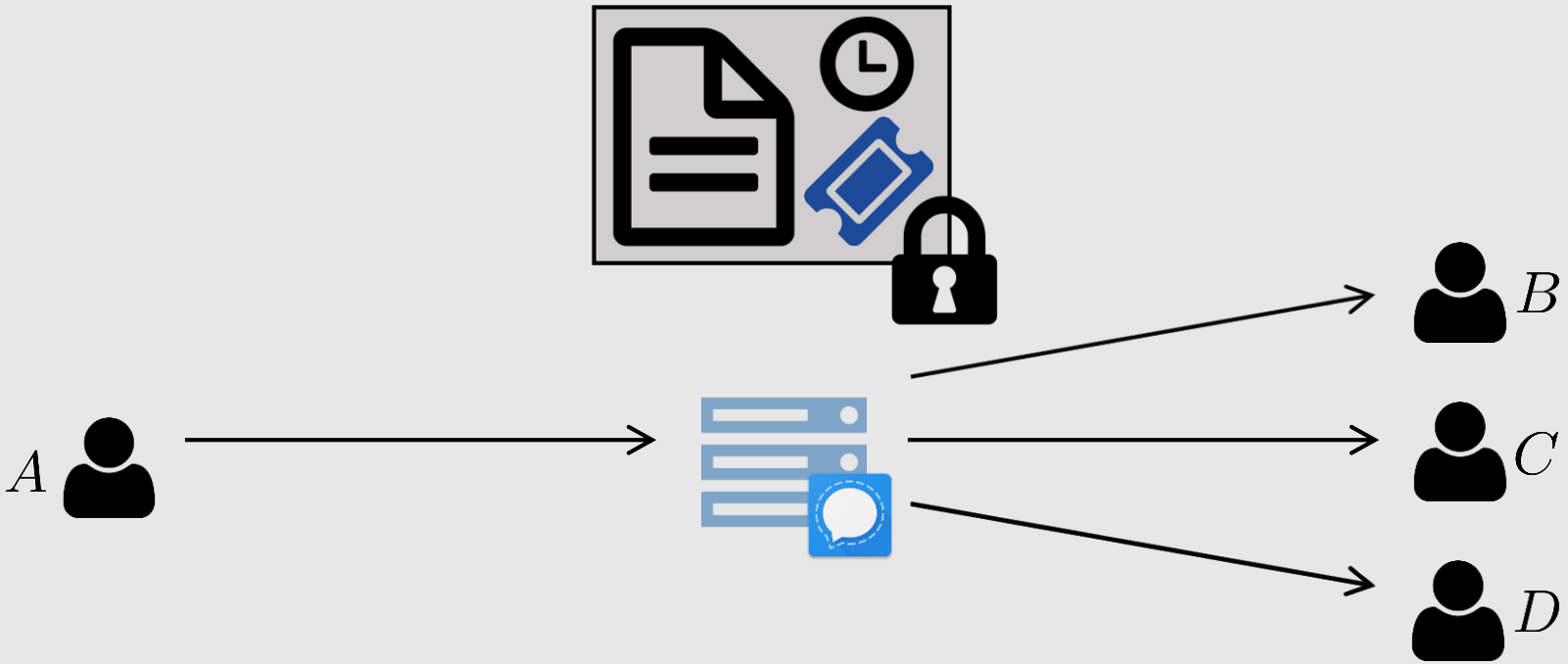
Protocol Overview: Signal

Protocol Overview: Signal

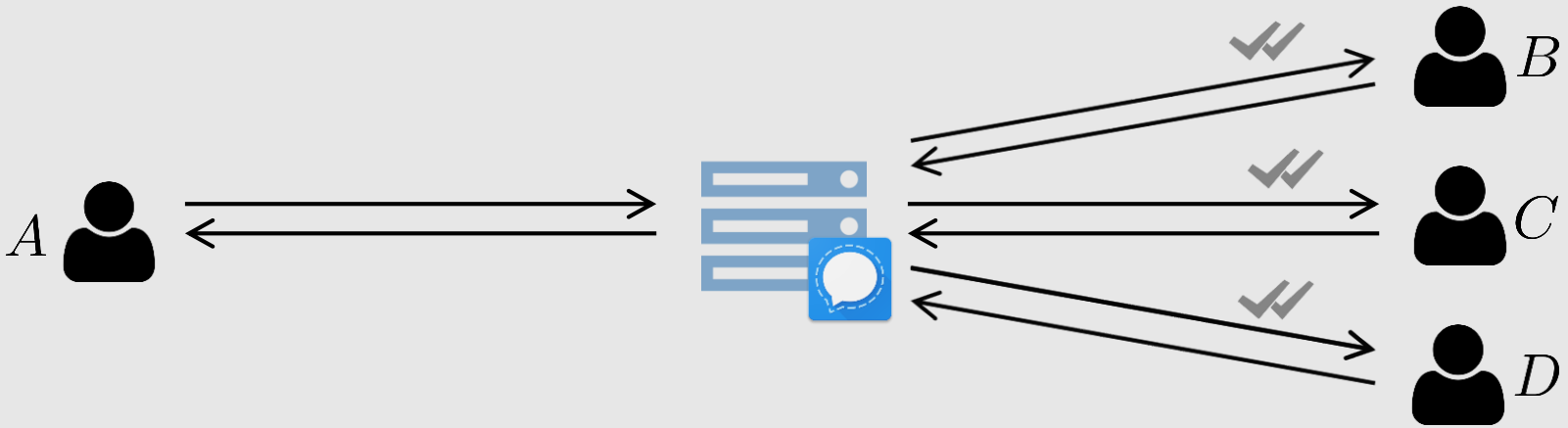
Protocol Overview: Signal



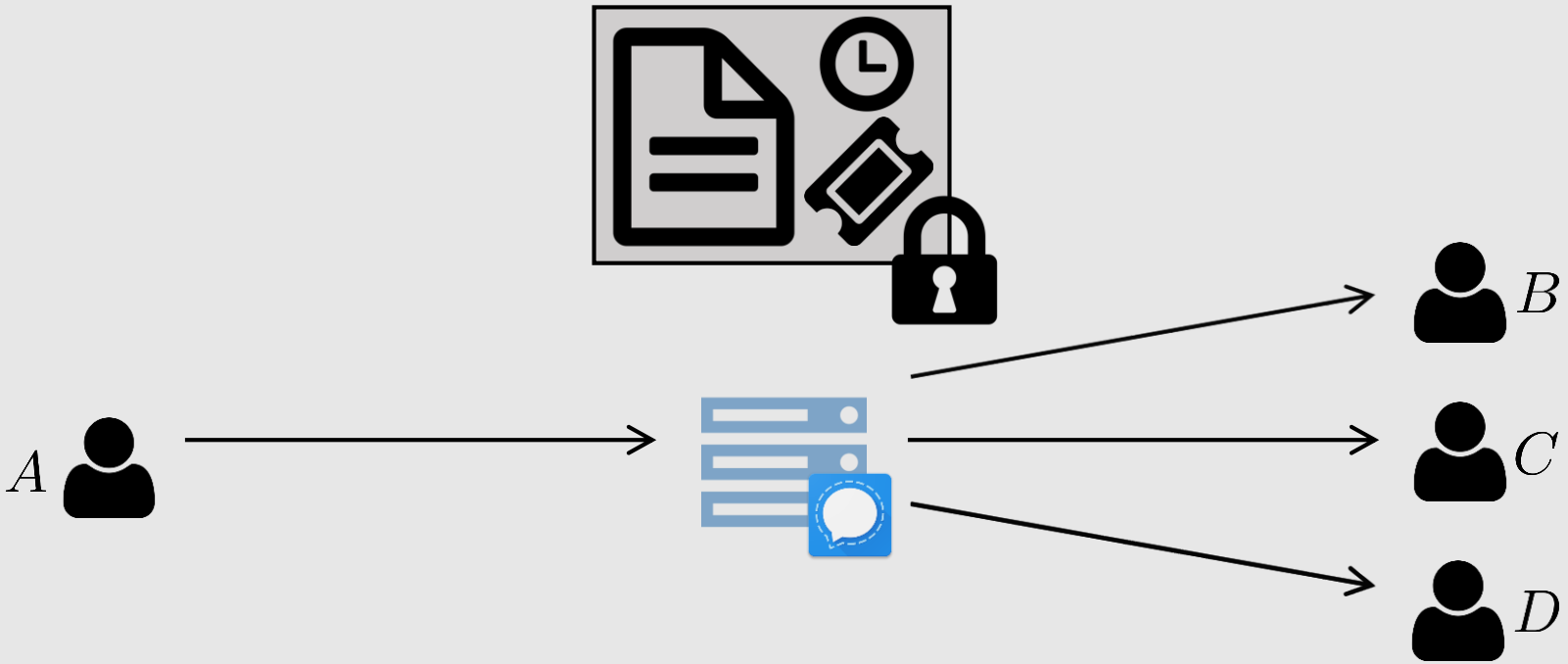
Protocol Overview: Signal



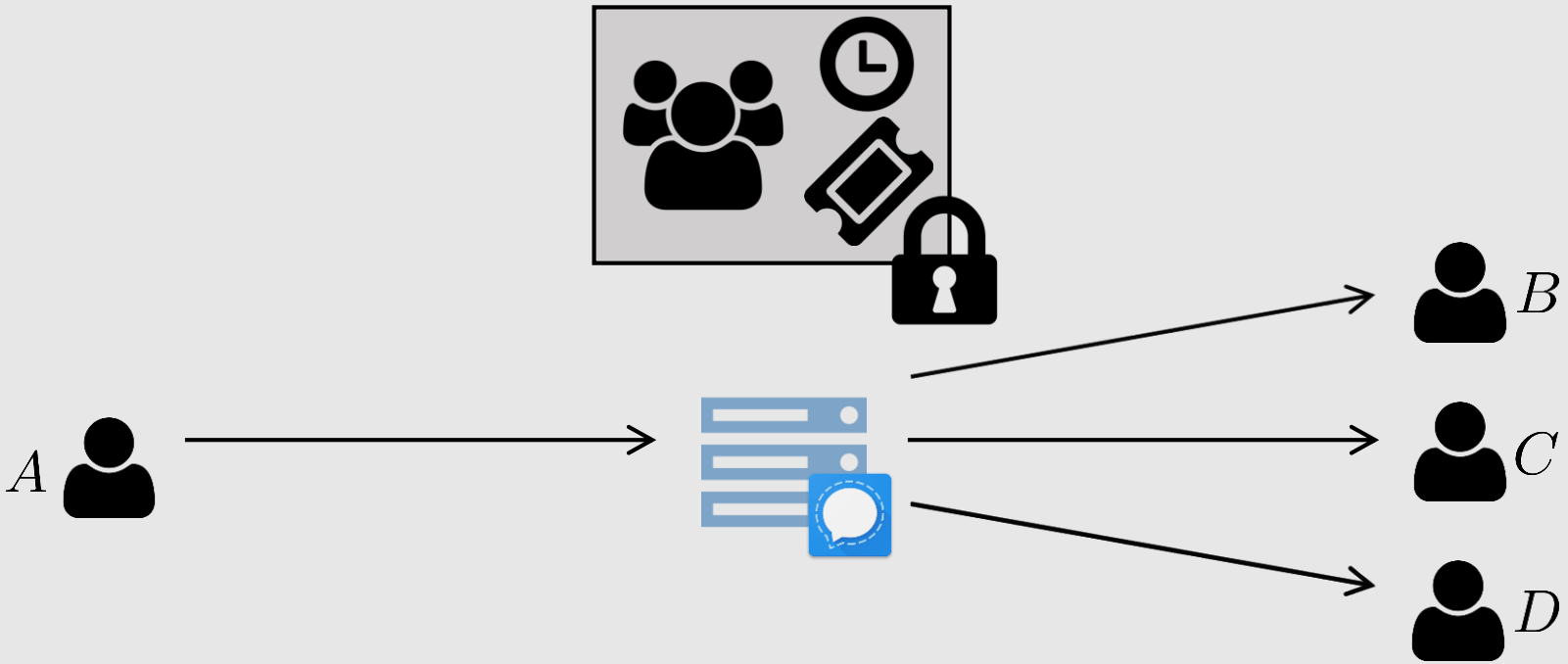
Protocol Overview: Signal



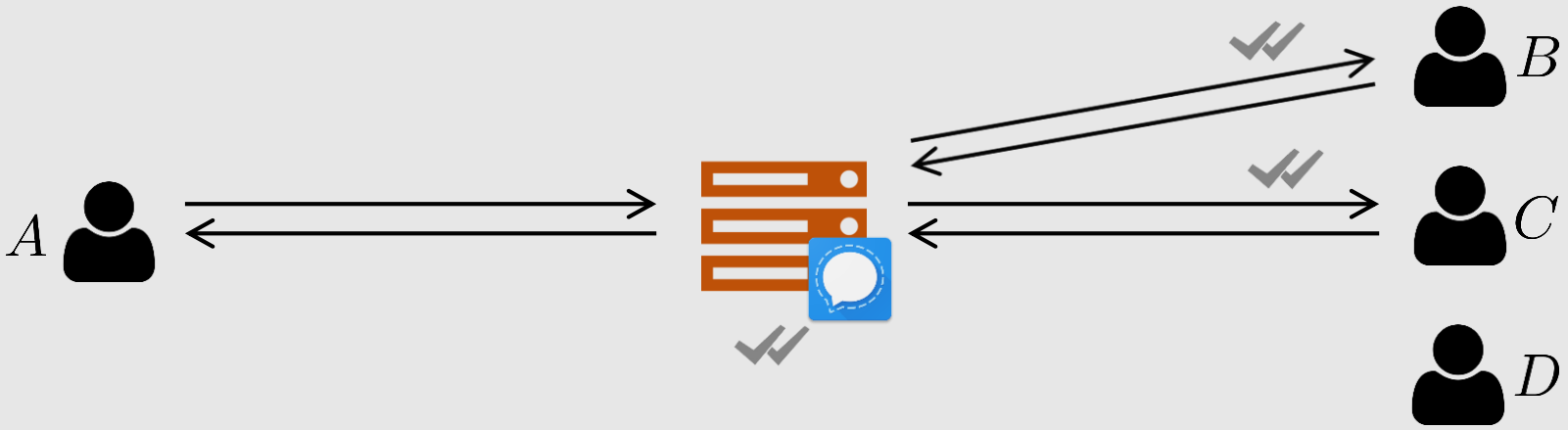
Protocol Overview: Signal

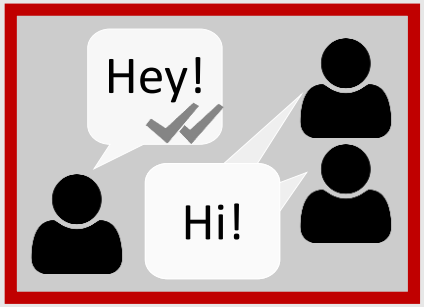


Protocol Overview: Signal

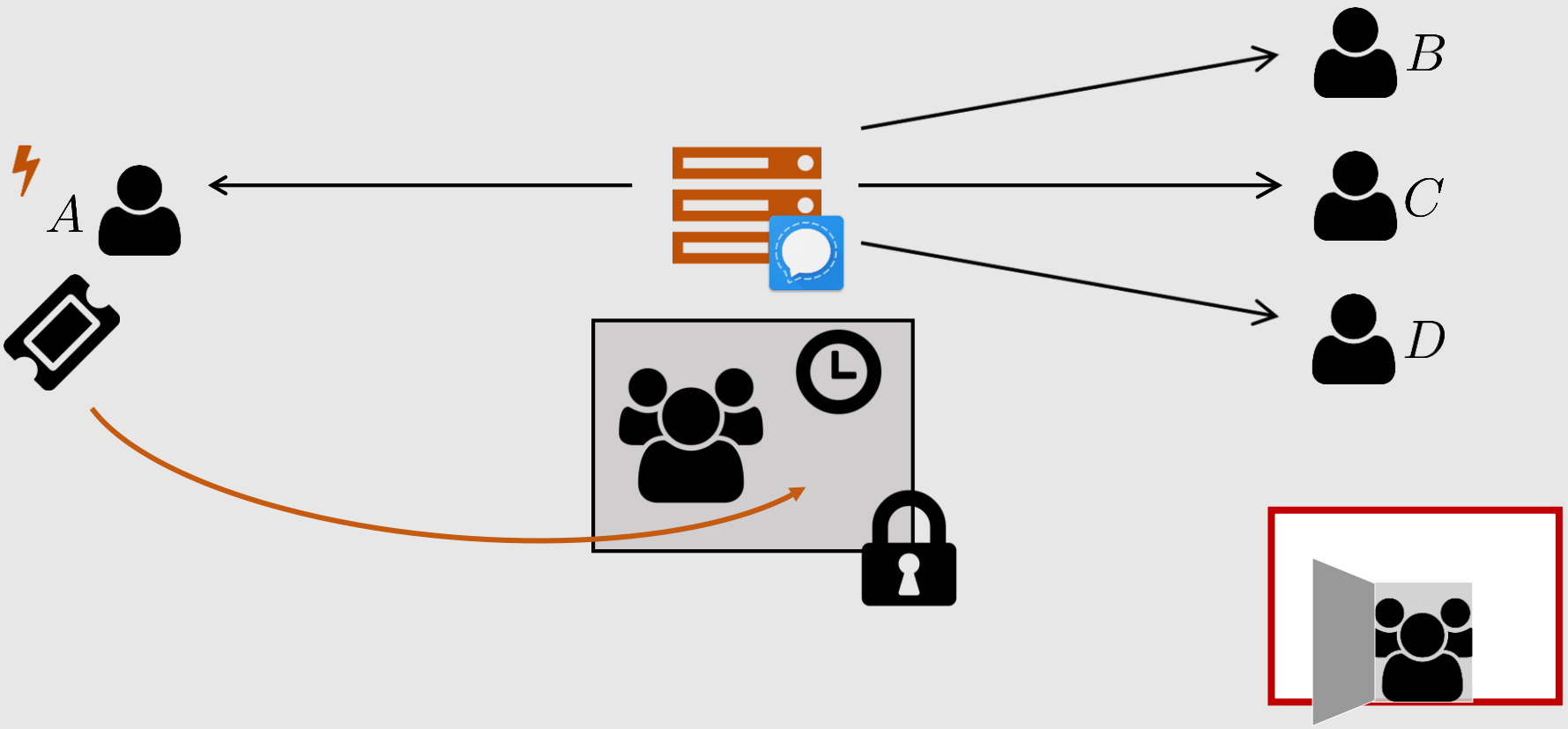


Weaknesses: Signal

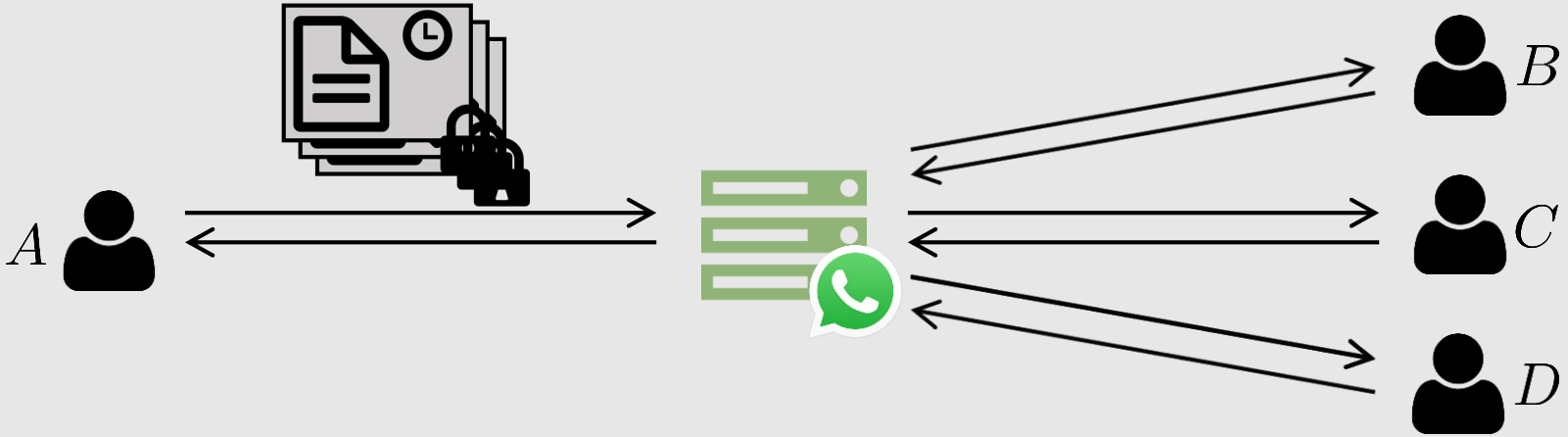




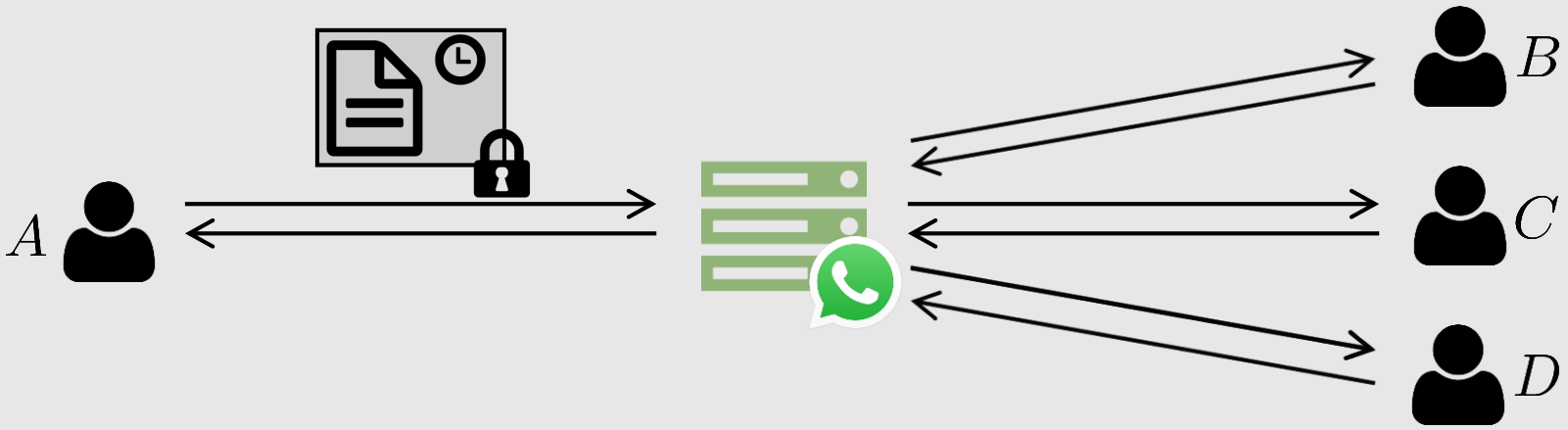
Weaknesses: Signal



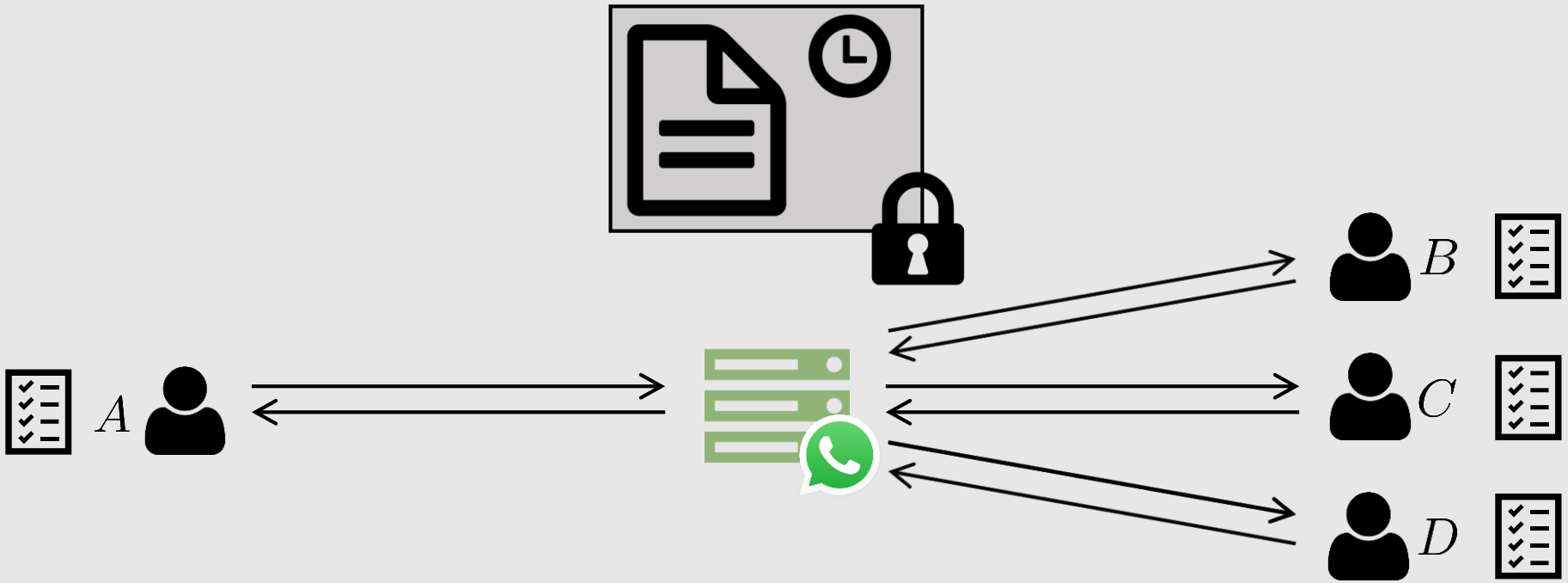
Protocol Overview: WhatsApp



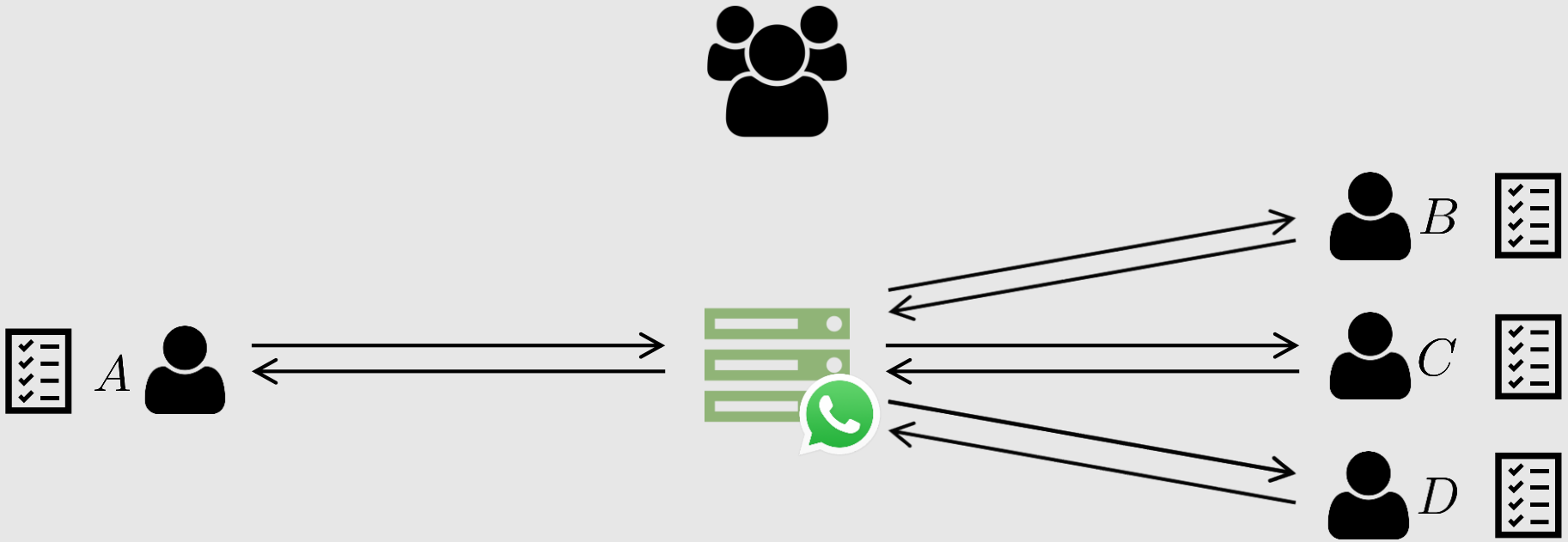
Protocol Overview: WhatsApp



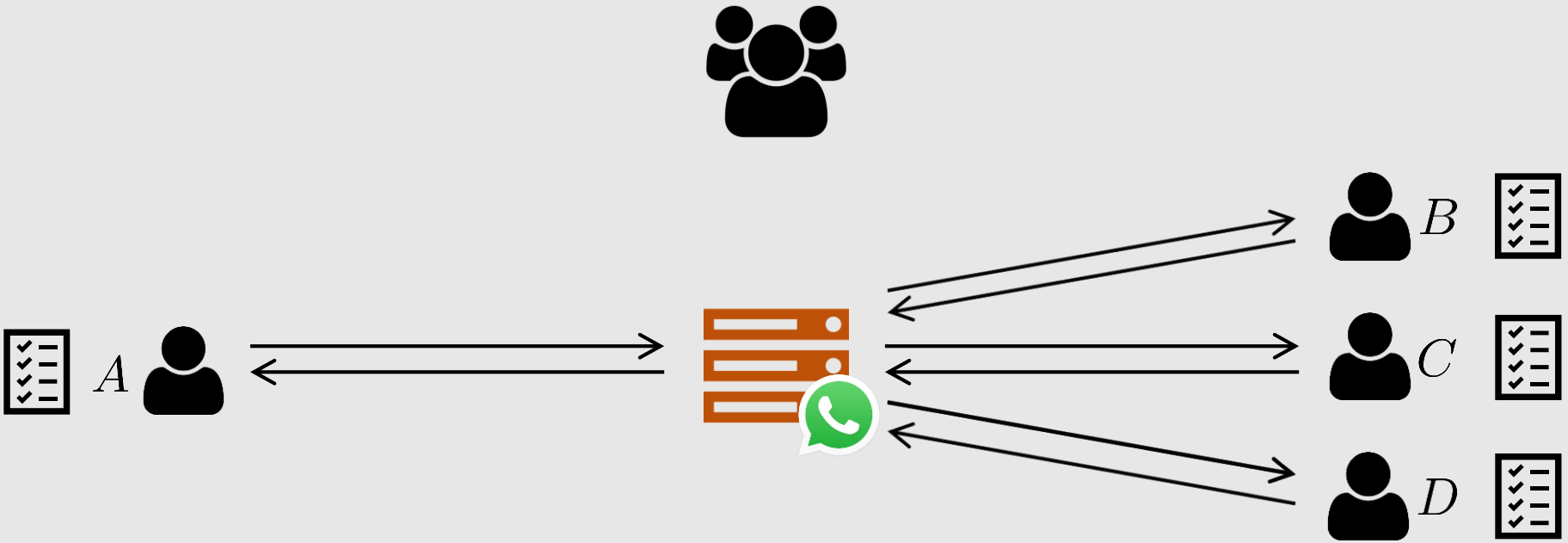
Protocol Overview: WhatsApp

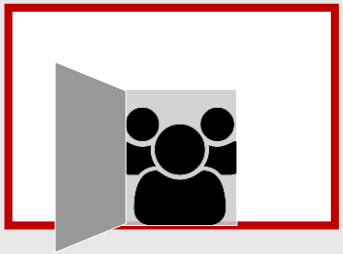


Protocol Overview: WhatsApp

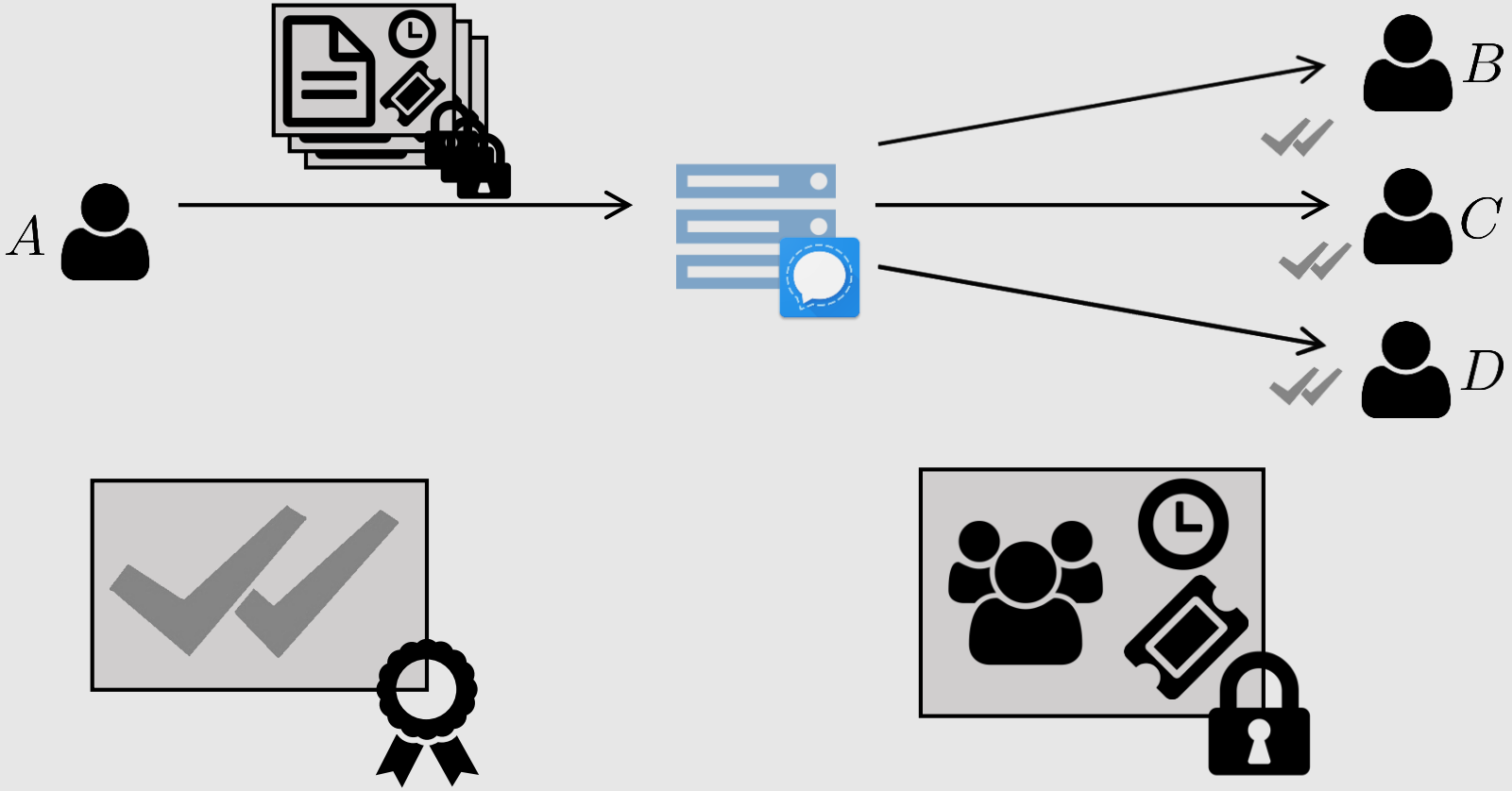


Weaknesses: WhatsApp

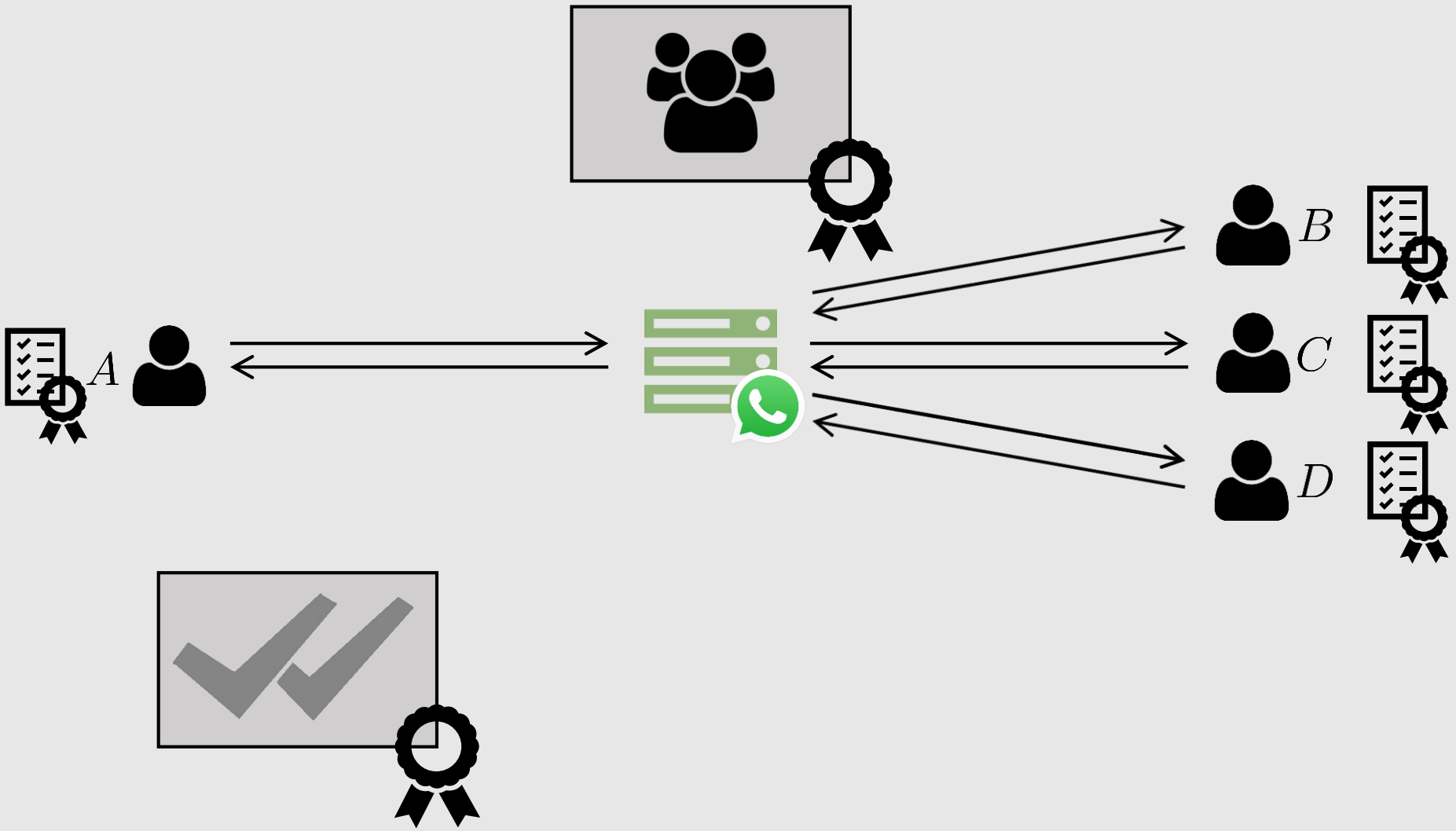




Enhancements: Signal



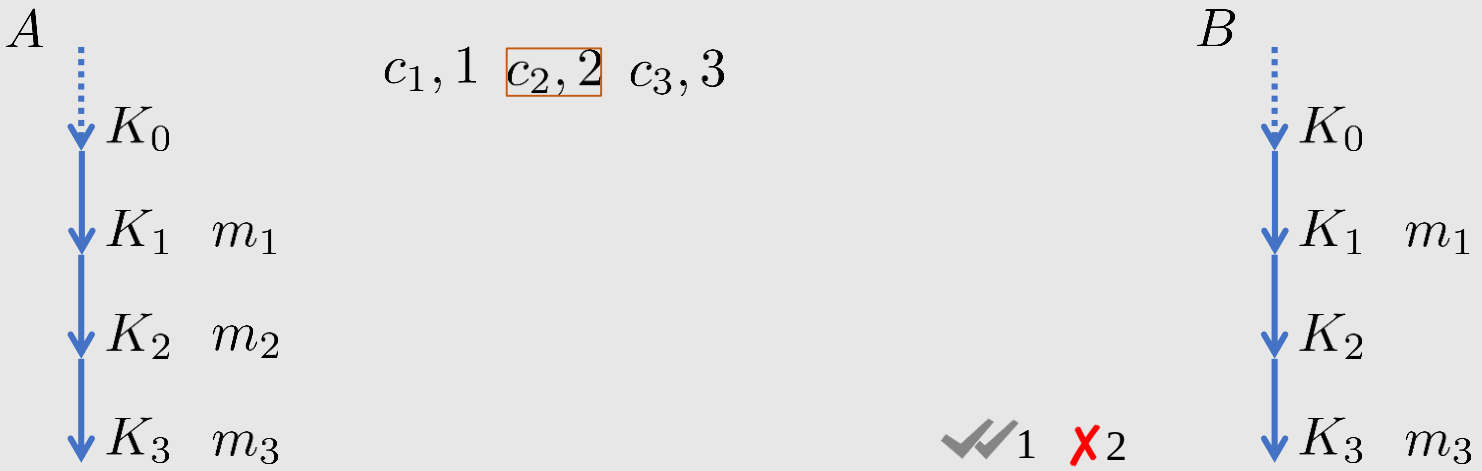
Weaknesses: WhatsApp



Solutions: Traceable Delivery

- For Signal and WhatsApp with key stream (stateful encryption):
  - Key omissions in key stream are ignored

→ Ack newest in order received message (e.g., with content messages)
→ Send negative ack (NACK) on key omission



Summary

- First security model for group instant messaging
  - Captures security and *reliability*
- Description (⇒ reverse engineering) of three major IM protocols
- Application of model to protocols
  - Revelation of discrepancies between security definition and protocols:

	Closeness	Forward Secrecy	Future Secrecy	Traceable Delivery	No Duplication	No Creation
	✓		✓	✓		✓
	✓		✗	✓		✓
	✓	✗	✗	✗	✓	✓

  - Probably not the only protocol/implementation weaknesses
  - Signal still **very** secure! WhatsApp brought E2E encryption to 10^9 users!

ia.cr/2017/713 **@roeslpa**