privacy
Winfried
Tilanus
e-health
information
system
patient
identity
data
analysis
relation
relationship
healthcare
treatment
practitioner
control
automated
patients
definition
research
interventions
MEDDEV
WGBO
surveillance
ethical
society
environment
part
must
care
tailored
inside
medical
within
safe
social
systems
public
relationships
become
directive
tailoring
two
third
new
like
paper
approach
user
digitalization
ability
Also
demands
limited
might
way
edge
much
example
problem
party
individual
panopticons
also
people
potential
using
take
concept
different
large
software
influence
case
behavior
processes
something
behaviour
without
normative
patterns
time
understand
question
relations
power
process
panopticon
possible
lot
kind
quite
becomes
one
bubble
clear
legal
forced
autonomy
positioning
many
often
online
techniques
amount
results
certain
context
look
active
expectations
health
records
able
makes
always
expect
level
help
problems
evidence
informed
better
customers
want
done
digital
limits
used
consent
created
make
implications
see
try
scale
may
organizations
events
big
even
less
first
use
second
based
need
intervention
somebody
quality

The hairy issue of end-to-end encrypted instant messaging

Winfried Tilanus
xmpp:winfried@tilanus.com
mailto:winfried@tilanus.com

Fosdem’20 2020-02-01

About me

- 20y experience with messaging in (health)care
- Member of XMPP Standards Foundation
  - Seen 4 standards for end-to-end-encryption
- This is not an opinion of the XSF

This talk:

- Threat model issues with E2EE
- Practical issues with E2EE

Encrypting Messaging

- Connection encryption:
  - Decrypted and re-encrypted at servers
  - Servers process messages in plaintext
  - Servers need routing information
- E2E encryption:
  - Decrypted at endpoints
  - Servers still need routing information

Added value of E2EE?

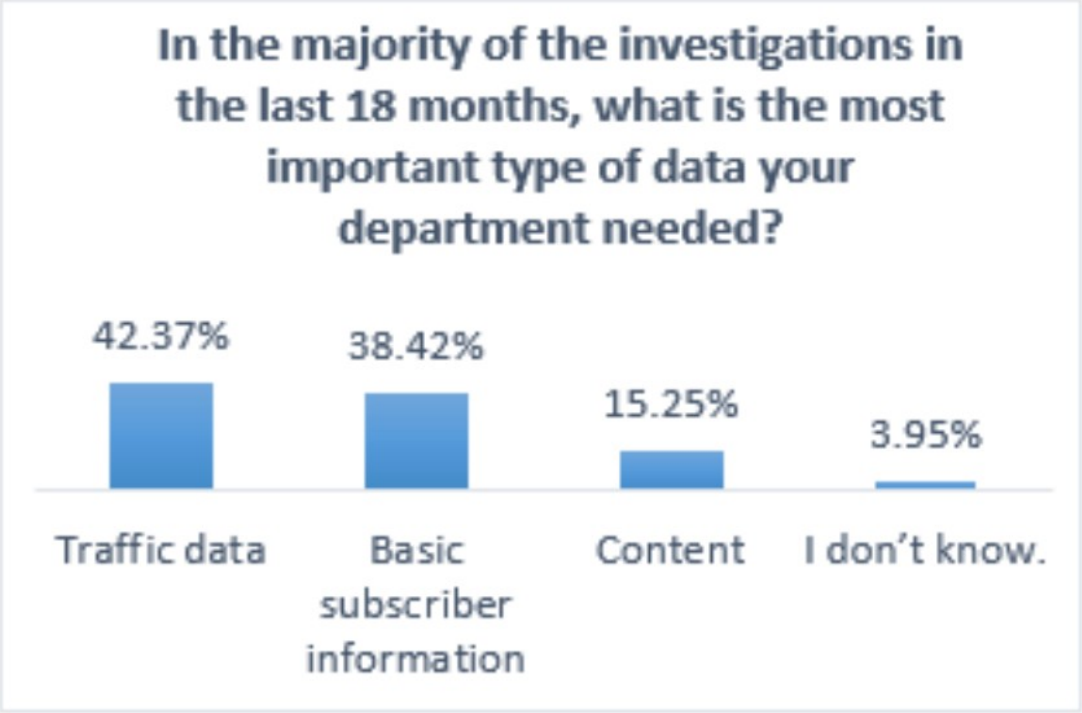
- Not decrypted at hops
- Useful when you don’t trust your servers
- But you still have to trust your servers with metadata for routing

Attack scenarios

- Secret service performing large scale monitoring
- Big tech company analysing messages for advertisement

Secret service attack

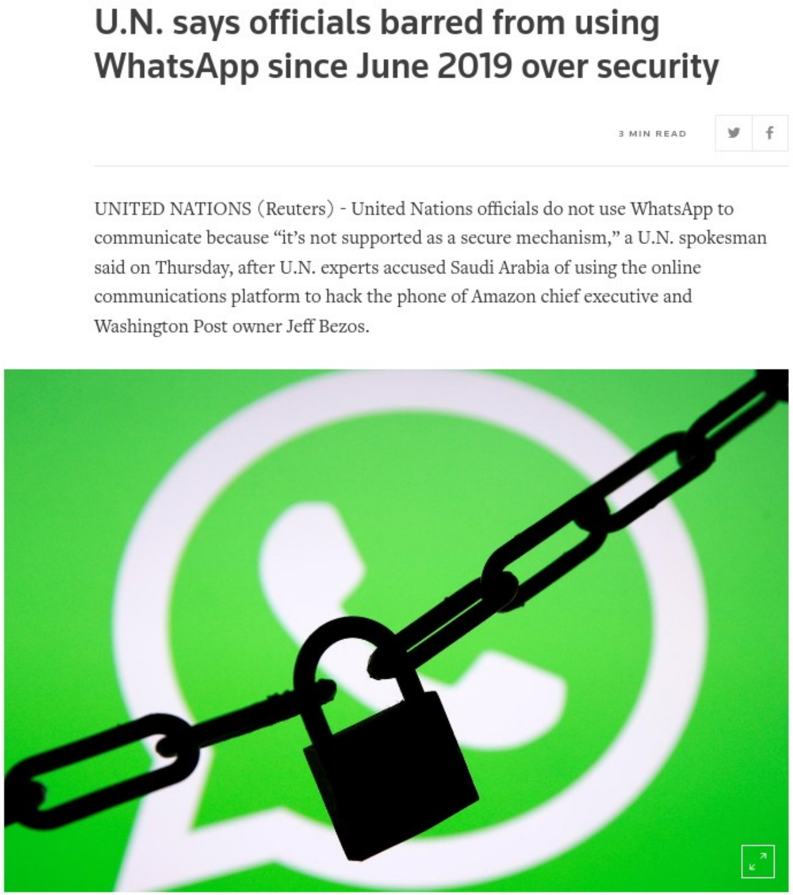
- Steps:
  - Attention
  - Analyse network (metadata)
  - Option 1: tap
  - Option 2: hack



Source:
Europol SIRIUS EU Digital Evidence Situation Report 2019 (p.16)

Secret service attack (2)

- E2EE hardly protects
- Hacking is attractive anyway



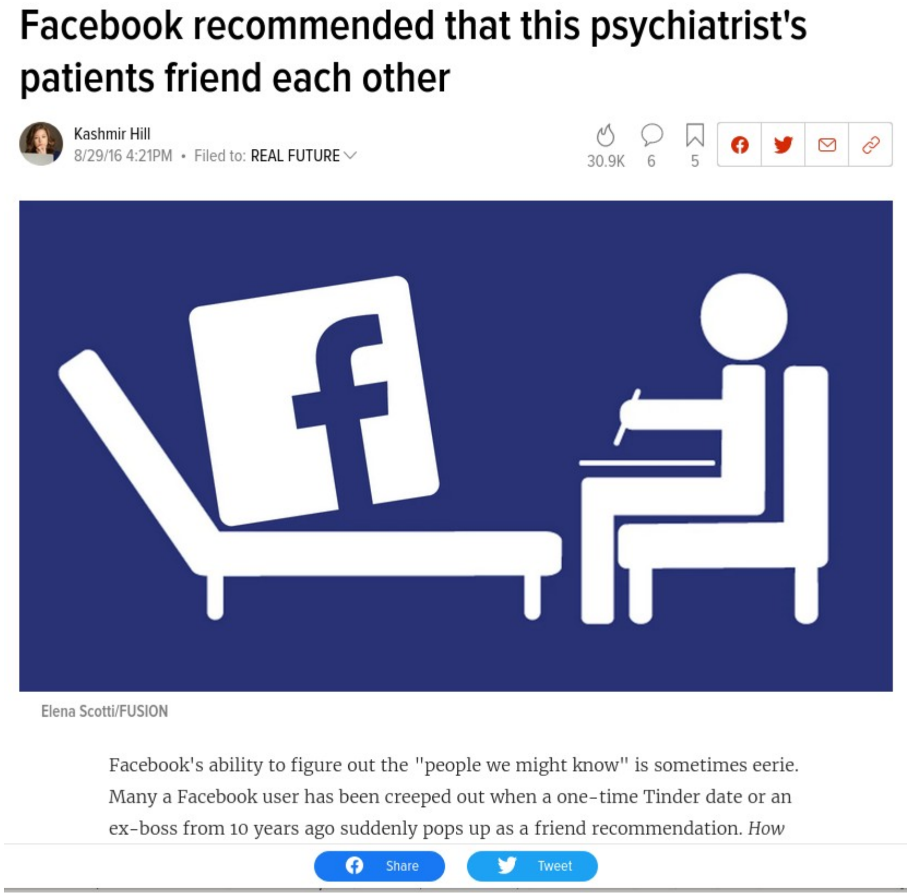
U.N. says officials barred from using WhatsApp since June 2019 over security

UNITED NATIONS (Reuters) - United Nations officials do not use WhatsApp to communicate because “it’s not supported as a secure mechanism,” a U.N. spokesman said on Thursday, after U.N. experts accused Saudi Arabia of using the online communications platform to hack the phone of Amazon chief executive and Washington Post owner Jeff Bezos.

Source: Reuters, January 23, 2020

Big company attack

- Map social graph
- Assume properties
- Sell advertisement



Facebook recommended that this psychiatrist's patients friend each other

Kashmir Hill
8/29/16 4:21PM • Filed to: REAL FUTURE

Elena Scotti/FUSION

Facebook's ability to figure out the "people we might know" is sometimes eerie. Many a Facebook user has been creeped out when a one-time Tinder date or an ex-boss from 10 years ago suddenly pops up as a friend recommendation. *How*

Big company attack (2)

- Only metadata
- E2EE is useless

Attack model issue

E2EE does not protect against surveillance.

But E2EE can be effective

Works for server operators:

- Against law enforcement
- When using (cloud)infrastructure

What is E2EE for?

E2EE without metadata protection does not protect end users.

It protects server operators

Part 2: practical issues

- Storage and forward
- Audit trails & archiving
- Group chats & multiple devices
- Key verification

Not solved well right now, but may be solvable

Store and forward

- Perfect Forward Secrecy = rotating keys
- Store and forward = stable keys

Trade-off

Audit trails and archiving

What is security?

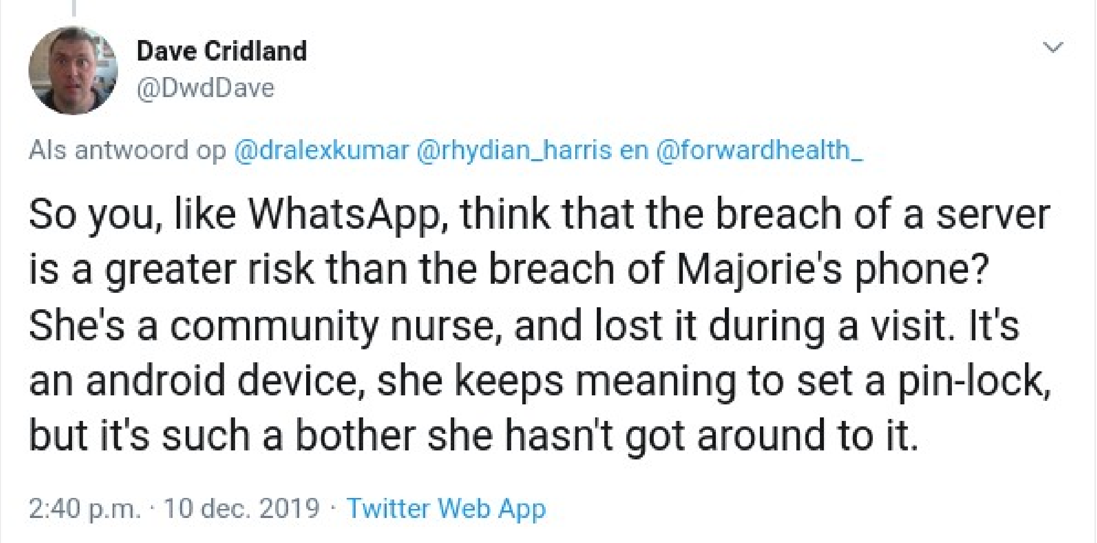
- Human rights activist:

  “no traces at all”

- Medical doctor:

  “archive, audit trail &

  no storage on device”



Dave Cridland
@DwdDave

Als antwoord op @dralexkumar @rhydian_harris en @forwardhealth_

So you, like WhatsApp, think that the breach of a server is a greater risk than the breach of Majorie's phone? She's a community nurse, and lost it during a visit. It's an android device, she keeps meaning to set a pin-lock, but it's such a bother she hasn't got around to it.

2:40 p.m. · 10 dec. 2019 · Twitter Web App

Creating an archive

- At endpoints or at server?
- Re-encryption to static key?
- Managing access?
- Proving integrity?

Our endusers do want E2EE; they also want nothing held on the device and a search function. You can imagine my fun.

David Cridland – Pando

One-to-many messages

Examples:

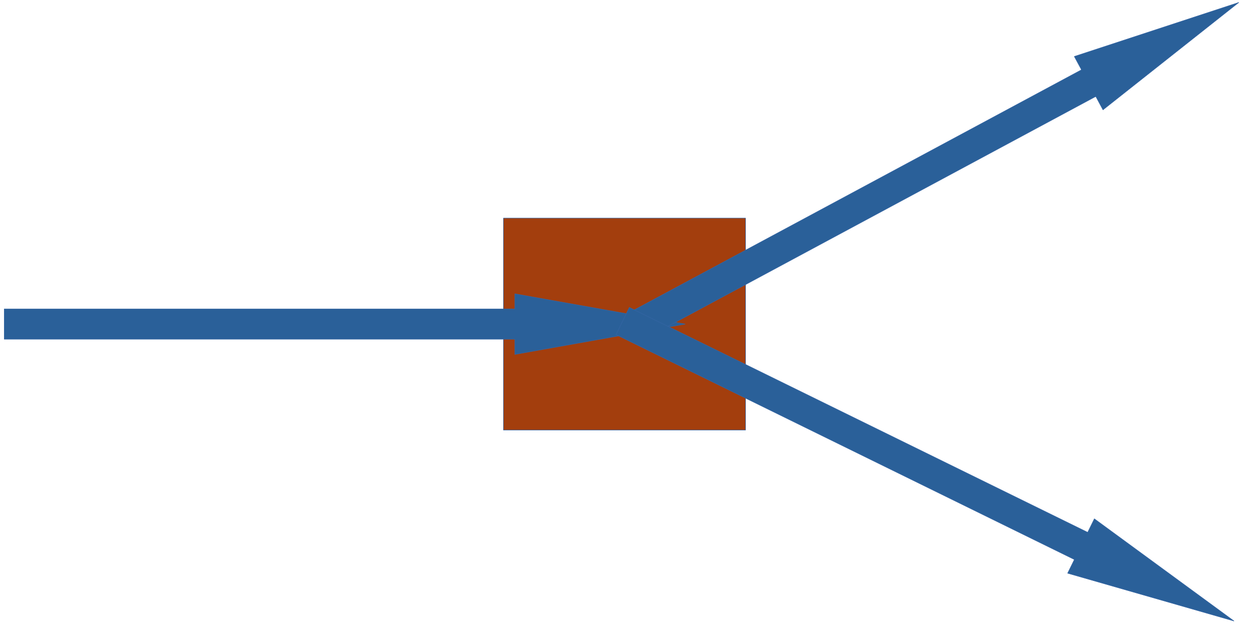
- Chat groups
- Syncing multiple devices

Common mistakes:

- Sharing secret key
- Encrypting to each endpoint

One-to-many messages

Ideal: re-encryption at server without decrypting



One-to-many messages

- Diffie-Hellman:
  - ‘Group-key’ from all keys
  - Adding keys
  - Removing keys
- IETF has draft: “Message Level Security” (MLS)
  - No reviewed & operational standard yet

Key verification

- Leap of faith?
- Web of trust?
- Trusted third party?
- Verification in person?
- Identity based cryptography?

Key verification (2)

- How to handle changes in keys?
- How to revoke keys?
- How to create trust between multiple devices?

Fail at key verification and your E2EE is useless

Conclusion

Bad encryption is better then no encryption

(Ian Goldberg)

or

Bad encryption is a false sense of security

Resources:

- Thanks to David Cridland
  - Read his blog “crypto show and tell” at: https://dev.to/dwd/
- Message Level Security:
  - https://datatracker.ietf.org/wg/mls/documents/
- Identity based cryptography:
  - https://www.ngi.eu/news/2019/08/20/user-friendly-email-encryption-possible-with-identity-based-cryptography/
- Metadata analysis resistant chats:
  - Briar: https://briarproject.org/
  - Katzenpost: https://katzenpost.mixnetworks.org/
  - Cwtch: https://cwtch.im/