Why Can't Online Social Networks Encrypt?

Ero Balsa, Filipe Beato, Seda Gürses

KU Leuven NYU

Workshop on Privacy and User–Centric Controls

20-21 November 2014, Berlin

PCWorld

Work. Life. Productivity.

NEWS | REVIEWS | HOW-TO | VIDEO | ...WARE | SECURITY | SC

Antivirus | Privacy | ...

<< Faceb... been **able to deploy end-to-end encryption** for a long time, Chi... ...fficer Joe Sullivan said on Tuesday. It hasn't rolled the tec... its services partly due to its **complexity**.>>

...before ...it

*The company has also held back because, wh... done right, it's **hard** for the average pe...*

*"If you use end-to-end encryption **on...***

10

Share

0

submit

and spies out ...

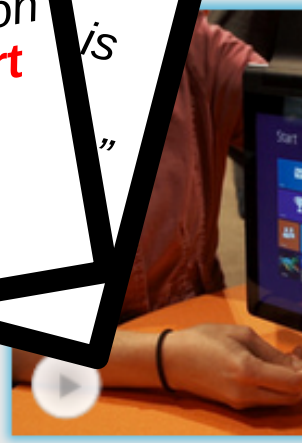
...is

...”

<<there are some third-party apps they can use to add end-to-end encryption to Facebook's services, Sullivan said. "At a **minimum**, we want to **support third-party initiatives**" he said>>

...the best way to secure users' ...major products by default. The technology is meant ...people's communications at their client devices so that governments and others must target the person and not Facebook's data centers.

VID...



Lenovo Yoga T...
It flips, folds ...

3 models of the OSN roles to provide/support E2EE

Key management.

Implementation/Usability Challenges.

Threat model.

Disclaimers:

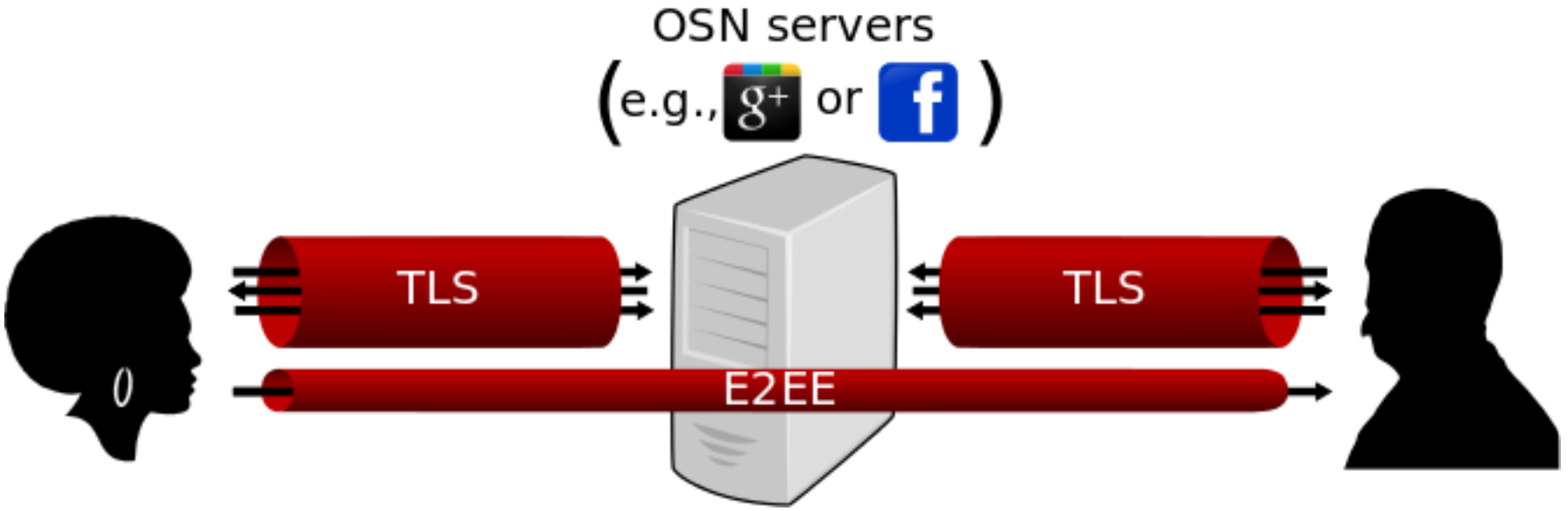
Work in progress!!

I'm not a cryptographer!!

A pragmatic stance.

E2EE on OSNs

- Encrypted from sender to recipient.



- (At least) For private messages.

- Other properties, e.g., Perfect Forward Secrecy?

Model 1:
OSN as PKI

- Key management: OSN is in charge.
  - Public keys: OSN is CA and key server.
  - Private keys: stored & managed by the user, with sync/restore mechanisms.
  - Can be made very convenient!

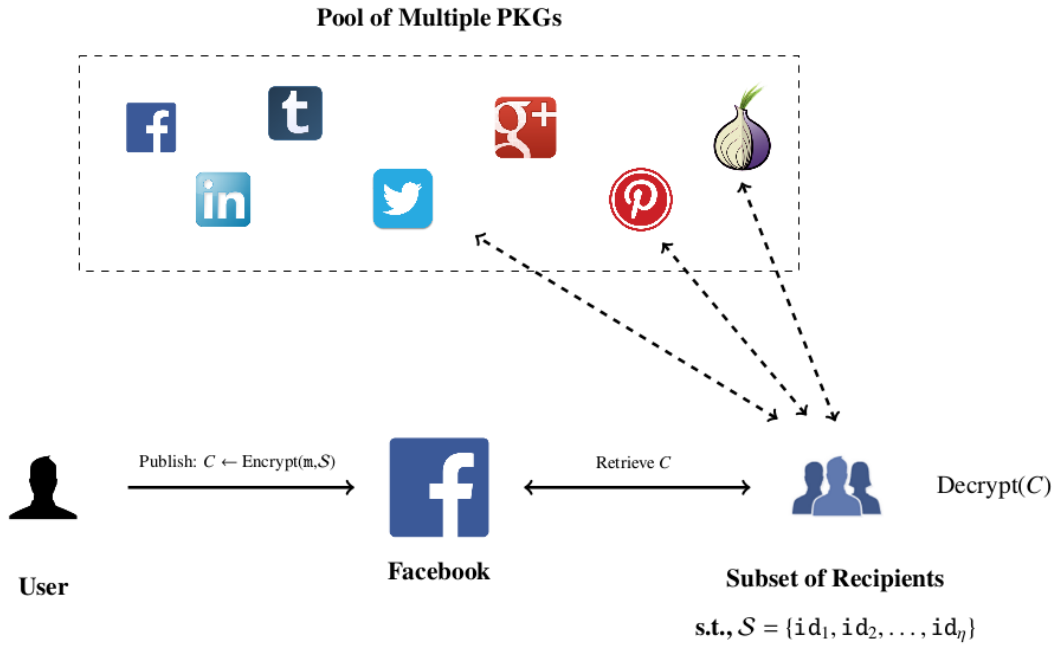
- Threats:

  OSN needs to be trusted!

  - As CA
  - As E2EE tool provider (backdoors?).

Model 2: OSN as Federated ID-Based PKG

- No trusted CA: Public key is a (human-readable) identifier.
- Private key: Distributed Key Generation (but still managed by the user).



Threats:

- Authorities collusion.
- Tool provider?

Model 3:
OSN as Supporter
(of 3rd party initiatives)

- Third-party browser plugins: PGP-like key management.
  - Public keys: uploaded to the OSN but authenticated by the users.
  - Private keys: stored and managed by the user.

- OSN cooperates with scarce-resources developers:
  - API for parsing, specific data fields.
  - Promotion, involved in testing.

- Threats (wrt the OSN):
  - OSN can DoS.
  - (Occasionally) MITM

Discussion (1/2)

- OSN as provider? Unacceptable!! Unless...
- A third party provider.
  For users, is this really better?
- Trade-off between convenience and security.
  No best way of implementing E2EE?
- For any tool:
  - Encryption on/off
  - “Compatible users” → “invite button”.

Discussion (2/2)

- It's the OSN's (moral) responsibility.
- Other actors?
  - Browser developers.
  - W3C's Web Crypto API?