Definition of End-to-end Encryption

https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition

Authors

- Mallory Knodel, Center for Democracy and Technology
- Fred Baker, ISC
- Olaf Kolkman, ISOC
- Sofia Celi, Cloudflare
- Gurshabad Grover, Centre for Internet and Society India

Goal

A priori definition of end-to-end encrypted communications.

History

Draft-00: Presented to MLS @ IETF 111

- Suggested to take the draft to secdispatch as e2ee is wider than MLS.

Draft-01: Presented to secdispatch @ IETF 112

- Formed new list: e2ee@ietf.org
- Several reviews, new issues.

Draft-02: Presenting to OpenPGP @ IETF 113

- More reviews.
- Interest in adoption?

Outcomes

Things that are not e2ee can’t easily be called e2ee.

Parallel drafting in MLS, OpenPGP to compliment existing drafts’ terminology.

Articulation of norms- and principles-driven implementations.

Anti-goals

Anti-definition.

Directly invoking threats in order to define e2ee.

Public record of discord and disagreement about what is e2ee.

TOC

1. Formal definition
    a. End
    b. End to end
    c. Encryption
    d. Succinct definition
2. System design
    a. Features
    b. Challenges
3. User expectations

Changes

Since -00

- Broke out separate subsection in the formal definition on “end”.

Since -01

- Nits and edits from Britta
- Added functional definition as a formal definition subsection from Chelsea
- Linked concept of identity and endpoint in first section

Future of the draft

- A few smaller issues still open
- Information around how metadata is best protected in end-to-end communications
- More ideas around forward secrecy and backwards security in regards to device compromise and disappearing messages
- Check deniability considerations text.

PRs, reviews welcome

https://github.com/mallory/e2ee