Exploring User Mental Models of End-to-End Encrypted Communication Tools

Ruba Abu-Salma (University College London)

Elissa M. Redmiles (University of Maryland)

Blase Ur (University of Chicago)

Miranda Wei (University of Chicago)

8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)

Our Main Message

Secure messaging has a messaging problem!

Introduction

- Our community has advocated the adoption of secure communication tools.
- These tools offer different security properties:
  - Confidentiality
  - Integrity
  - User authentication

Related Work

- Why Johnny Can’t Encrypt? A Usability Evaluation of PGP 5.0 (Whitten and Tygar, 1999)
- …
- Why Doesn’t Jane Protect Her Privacy? (Renaud et al., 2014)
- Obstacles to the Adoption of Secure Communication Tools (Abu-Salma et al., 2017)

Prior work has shown that incorrect mental models are a barrier to the adoption of secure tools.

In This Work

We **quantitatively** explore user mental models of end-to-end (E2E) encrypted communication tools.

Research Questions

- RQ1. What are users’ general mental models of E2E encryption?
- RQ2. Do users understand the security properties offered by E2E encrypted communication tools?

Soteria: A Hypothetical E2E Encrypted Tool

Imagine you are considering using a new tool named Soteria to communicate with your family members, friends, colleagues, and others. When you install Soteria, the following message is displayed:

“Soteria communications (messages, phone calls, and video calls) are end-to-end encrypted.”

Survey Topics – Mental Models (RQ1)

- Have you heard of the term “end-to-end encryption?”
- Do you feel confident explaining what it means?
- What does end-to-end encryption mean to you?
- What do the ends in “end-to-end encryption” refer to?
- What are the benefits and drawbacks of using Soteria?
- Do different types of communication have the same level of security?

Survey Topics – Security Properties (RQ2)

- Which of the following entities could access your Soteria communications?
  - People who work at Soteria
  - People with a technical background
  - People who are up to no good
  - Corporations other than the company that develops Soteria
  - Governments
  - ISPs
  - Other
  - No one

Survey Recruitment

- Iteratively developed questionnaire.
- Conducted survey in the UK in April 2018.
- Recruited 125 survey respondents using Prolific Academic.
- Paid each respondent £2.5.
- Average completion time = 10 minutes.

Data Analysis

- Two researchers coded qualitative responses using Thematic Analysis.
- Cohen’s kappa coefficient = 0.87.

Results – Demographics

♀ ♂

58% 40%

Age

18 – 44: 80%

Educational level

College degree: 34%

Graduate degree: 20%

Results – Demographics

90%

Use (or used) E2E encrypted tool

Results – Demographics

90%

Use (or used) E2E encrypted tool

87%

Use (or used) WhatsApp

Results – Demographics

62%

Had heard of E2E encryption

Results – Demographics

62%

Had heard of E2E encryption

12%

Felt confident explaining E2E encryption

Results – General Mental Models

- Benefits?

86%

Provides E2E encryption

Results – General Mental Models

- Benefits?

86%

Provides E2E encryption

- Drawbacks?

11%

Partners need to use Soteria

9%

Cybercrime

Results – General Mental Models

- What does E2E encryption mean?

34%

No one could access

33%

Only sender and recipient could access

5%

Only devices could access

Results – General Mental Models

- What do the ends refer to?

50%

Sender and recipient

30%

Devices/instances

Results – General Mental Models

- What do the ends refer to?

50%

Sender and recipient

30%

Devices/instances

15%

Start and end of exchanged message

Results – Security of Different Types of Communication

~70%

Same level of security (Soteria communications)

Results – Security of Different Types of Communication

~70%

Same level of security (Soteria communications)

~75%

Soteria text messages <= landline phone calls, mobile phone calls, SMS

Results – Access to Soteria Communications

~40%

No one could access

Results – Access to Soteria Communications

~40%

No one could access

~60%

At least one entity (governments, Soteria employees, technical people) could access

Results – Access to Soteria Communications

~40%

No one could access

~60%

At least one entity (governments, Soteria employees, technical people) could access

~75%

Were not confident

Our Main Message

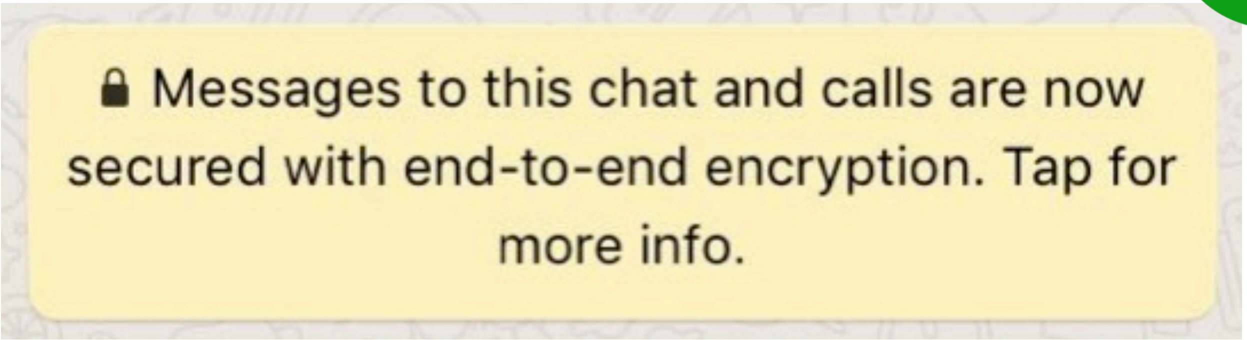
Secure messaging has a messaging problem!

Key Takeaways

- Users might not feel threatened by proposals of "backdoors."
- Primary user-related challenge for E2E encrypted tools is appropriate use, not adoption.

Hypothesis

- A high-level description of a secure communication tool as “end-to-end encrypted” does not provide users with the necessary information.



🔒 Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

Recommendations

- Designing better descriptions to communicate the security properties of E2E encrypted communication tools, and increase users' feelings of self-efficacy.

Recommendations

- Designing better descriptions to communicate the security properties of E2E encrypted communication tools, and increase users' feelings of self-efficacy.
- Developing educational interventions targeted towards activists, dissidents, and policy makers.

Recommendations

- Designing better descriptions to communicate the security properties of E2E encrypted communication tools, and increase users’ feelings of self-efficacy.
- Developing educational interventions targeted towards activists, dissidents, and policy makers.
- Focusing on appropriate use, not adoption.

Exploring User Mental Models of End-to-End Encrypted Communication Tools

Ruba Abu-Salma (University College London)

Elissa M. Redmiles (University of Maryland)

Blase Ur (University of Chicago)

Miranda Wei (University of Chicago)

8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)