Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study

Wei Bai, Michael Pearson, Michelle L. Mazurek (University of Maryland, College Park)
Patrick Gage Kelley (Google LLC)

The 5th European Workshop on Usable Security (EuroUSEC), 2020
End-to-End Encryption (E2EE)

Hackers
Governments
Misbehaving Employees/Company Itself
Incorrect mental models of E2EE inhibit **confident**, **proactive** and **correct** usage.
Incorrect Mental Models Inhibit Usage

- People perceive E2EE incorrectly in both directions.
- Difficult for users to make thoughtful decisions.
- Struggled to complete some E2EE tasks.

Goal: Help people grok basic understanding and threats

- **Enough** to make judgments about how to communicate
- **Without** turning everyone into crypto experts
- **Naturally** when using the app (e.g., interstitial messages)
- **Without** requiring people to sign up for training module
Initial Study: Method

Focus: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area
Initial Study: Method

**Focus:** What is important, what is surprising, what to convey to others
- 25 non-expert participants, DC area

Reasons behind quiz answers
Initial Study: Method

**Focus**: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area

Important, surprising, worth conveying
Initial Study: Method

**Focus**: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area

Critique two existing explanations
Initial Study: Method

Focus: What is important, what is surprising, what to convey to others
- 25 non-expert participants, DC area

Sample message of E2EE educational intervention
Modular Tutorial

- High-level overview
- Risks
- Common misconceptions
- High-level description of how it works

Non-Goal: design optimal in-person tutorials

- Not to evaluate our tutorials
Confidentiality: Most Significant

- Even though less surprising, participants found it important
- Some subtleties were surprising
  - ISPs are in the message path?

“... the internet service provider and the app company ... may still get a copy of the message, that is protected by this wall, that is nearly impossible to break. So they can see you sent a message, but they can’t see what the message says.”
Particularly like comparison of E2EE vs. non-E2EE
• Important to clarify weaknesses of E2EE as well as benefits

“Knowing the risks of the non-E2EE and then really comparing it to how is this better... that’s really the most important.”
Integrity & Authenticity Still Confusing

- Authenticity is conflated with username/password

“E2EE protects against message modification and impersonation. Not even usernames and/or passwords can be stolen or guessed.”
Takeaways

● Confidentiality: Most significant

● Explaining risks clearly is useful
  ○ Comparing E2EE vs Non-E2EE
  ○ Weaknesses

● Some pieces may not worth mentioning
  ○ Integrity & authenticity