Lab: Private Communication

Daniel Bosk

March 25, 2019

Abstract

The more our society depends on digital systems, the more important private communication becomes. We need private communications to sustain democracy, thus we need it to be available to everyone. The purpose of this laboratory work is to introduce some practical aspects of private messaging. More specifically, after it, you should be able to

- *apply* (securely!) some common implementations of cryptography for private communication — also including any set-up (e.g. key verification).
- *analyse* different systems for private communication based on their security properties and *evaluate* which is suitable in a given situation.
- *evaluate* different implementations of private communication from a usability perspective.

The topics of this assignment are: usability [1, Ch. 2] and cryptography [1, Ch. 5] and privacy-enhancing technologies [1, Ch. 23.4]. We then rely on the "Why Johnny can't encrypt" papers:

- "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." [5],
- "Why Johnny still can't encrypt: Evaluating the usability of email encryption software" [4],
- "Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client" [3],
- "Can Johnny finally encrypt?: evaluating E2E-encryption in popular IM applications" [2].

1 Introduction

In this lab we will evaluate some tools for private communication, in particular, email and instant messaging.

Email security has the longest history, this has been around since the 80s. Have they gained wide-spread adoption yet? No. There are two competing approaches: Pretty Good Privacy (PGP) and S/MIME. But there are alternatives coming, e.g., ProtonMail made the headlines a few years ago.

The security of instant messaging looks better than that of email. This is largely due to the extensive use of smartphones for messaging. There are apps such as Signal, WhatsApp (uses Signal's protocol) and a few more. Have they gained wide-spread adoption yet? More than for email.

2 Assignment

The assignment is divided into two parts, the first focuses on email and the second on instant messaging.

2.1 Email security

List the security (and privacy) expectations that you have on email. Try to install and use a tool (e.g., GPG, ProtonMail, etc.) that achieves those expectations, or comes as close as possible, for securing an email conversation with a friend.

2.2 Instant-messaging security

List the security (and privacy) expectations that you have on instant messages. (Are they different than for email?) Try to install and use a tool (e.g., Signal, WhatsApp, etc.) that achieves those expectations, or comes as close as possible, for securing a conversation with a friend.

2.3 Reflection

What were the biggest problems that you encountered? What must be done to resolve them? Can they be resolved?

Read the "Why Johnny can't encrypt" papers which has studied exactly this problem throughout the years:

- "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." [5],
- "Why Johnny still can't encrypt: Evaluating the usability of email encryption software" [4],
- "Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client" [3],

all concern email, whereas "Can Johnny finally encrypt?: evaluating E2E-encryption in popular IM applications" [2] concerns instant messaging.

What problems did they find? What methods did they use?

3 Examination

Note down your thoughts from reading, experimenting and the reflections for the questions above and bring to the seminar session.

References

[1] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: `http://www.cl.cam.ac.uk/~rja14/book.html`.

[2] Amir Herzberg and Hemi Leibowitz. "Can Johnny finally encrypt?: evaluating E2E-encryption in popular IM applications". In: *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. ACM. 2016, pp. 17–28.

[3] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. "Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client". In: *arXiv preprint arXiv:1510.08555* (2015).

[4] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. "Why Johnny still can't encrypt: Evaluating the usability of email encryption software". In: *Symposium On Usable Privacy and Security*. 2006, pp. 3–4.

[5] Alma Whitten and J Doug Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In: *USENIX Security Symposium*. Vol. 348. 1999.