Week 13: Email encryption // more on teaching privacy

August 29, 8:30 am Pacific/11:30 am Eastern

Overview

This week, software developer Yakira Dixon will give us a brief overview of email, how it is insecure by default, and why encryption is necessary for secure communication. Then they'll discuss tools for encrypting email and their benefits and caveats. We'll then return to our week 5 concept of threat modeling, thinking through teaching strategies for teaching different groups in our community.

Learning objectives

- Learn about how to make email communication safer with encryption tools and better providers
- Learn about some of the usability and security issues that exist with end-to-end encrypted email

Readings

EFF's Surveillance Self-Defense guide for email:
https://ssd.eff.org/en/module/communicating-others#5
Riseup email documentation: https://riseup.net/en/email
FSF email encryption guide: https://emailselfdefense.fsf.org/en/

Guest lecturer

Yakira Dixon of Thoughtworks

Discussion

- Discuss what you learned in this week's lecture and readings
- Discuss teaching strategies for email encryption

Assignment

- Make a Riseup email account and/or set up GPG on your email client, or;
- Make instructional slides for teaching email encryption, or;
- Make an outline for a program plan for teaching a class aimed at one particular threat model, or;
- Make an outline for a basic privacy training for staff, or;
- Continue working on one of your assignments from a previous week