Week 23: Metadata resistance

November 7, 8:30 am Pacific/11:30 am Eastern

Overview

Even when data is encrypted, it is still often possible to discover and infer a lot of information about the communication from the metadata around it e.g. Do you really need to decrypt a phone call to know the context of a call to a crisis hotline at 3 in the morning? Communications metadata is known to be exploited by various adversaries to undermine the security of systems, to track victims and to conduct large scale social network analysis to feed mass surveillance. In this lecture we will hear from Sarah Jamie Lewis, who will cover what metadata is, the different kinds of metadata that can be recovered from web browsing, common messaging applications (as well as phone calls and texting), and embedded in documents. She will also discuss mitigation strategies for protecting yourself and others against metadata analysis.

Learning objectives

- Learn what metadata is and what types of metadata are collected in common applications
- Learn mitigation strategies for protecting against metadata analysis

Readings

- Intro to Cwtch https://openprivacy.ca/blog/2018/06/28/announcing-cwtch/
- Surveillance resistance infrastructure [will have the link before class]
- The First Contact Problem - Getting to SecureDrop: https://mascherari.press/the-first-contact-problem-getting-to-securedrop/ - How metadata in network traffic can deanonymize a source.
- We Kill people based on metadata (https://www.youtube.com/watch?v=UdQiz0Vavmc)

Guest lecturer

Sarah Jamie Lewis, director of Open Privacy Research Society

Discussion

Why does metadata matter?

Assignment

If you have an Android, download Briar: https://briarproject.org/
If you feel comfortable with running the prototype command line client for Cwtch, follow the instructions here: https://cwtch.im

Otherwise, continue work on final assignments.