Measure of the Impact of a STEM-Student-led Course on Privacy Enhancing Technologies for a non-Technical Target Population

Gunnar Wolf
Instituto de Investigaciones Económicas UNAM
Facultad de Ingeniería UNAM
gwolf@gwolf.org

Alejandro Miranda
Facultad de Estudios Superiores Iztacala UNAM

ABSTRACT

We present the results of a course on privacy-enhancing technologies (PETs) given by undergraduate students in the group we coordinate to a group of non-technical population, focusing on the attitude changes observed in the participants. This work was done as part of the UNAM/DGAPA/PAPIME PE102718 project, where we aim at explaining in a clear, simple language the need for PETs, dispelling the overwhelming perception that privacy and anonymity are unattainable for the *regular user*. The presented study is based on three applications of the survey completed by our first cohort.

CCS CONCEPTS

• **Security and privacy → Pseudonymity, anonymity and untraceability**; **Privacy-preserving protocols**; **Social aspects of security and privacy**; *Usability in security and privacy*; • **Social and professional topics → Privacy policies**; **Surveillance**; *Informal education*; *Computing literacy*; *Censorship*.

KEYWORDS

Privacy Enhancing Technologies, Non-technical population

1 BACKGROUND

Digital communication networks are a great enabler — For knowledge, for interpersonal contact, but also for pervasive spying and censorship by all sorts of actors, topping many dystopian social control predictions.

Numerous Privacy Enhancing Technologies (PETs) have been developed throughout the years, helping users escape the surveillance radar and providing privacy and anonymity. However, on one side, these tools have typically targeted technically inclined users, and are hard to use for the population at large; even worse, on the other side, some tools are published offering security guarantees they are incapable of attaining, giving users a false sense of security — and possibly putting them to a higher risk than they were already at to begin with. In the face of this, most non-technical users stay clear from PETs.

To improve on this situation, our project led STEM students to explore and understand different practices (personal information awareness) and PETs (privacy-oriented search engines, Firefox extensions and the Tor browser) and prepare a one week course they presented in a Social Sciences faculty, to a non-technical audience.

This poster presents the results gathered from three applications of a survey on the first cohort of this course: Before starting, at the end, and two months afterwards. The course was taught by three undergraduate Computer Engineering students, to a group of both teachers and students of the Social and Political Sciences Faculty of UNAM (Mexico).

2 METHODS

We started a study program that seeks to tackle this issue and bridge the gap to the general population. Throughout 2018 we coordinated a group of Computer Engineering undergraduate students to get them to understand the most important PETs. This included exploring the most common such technologies, building embedded infrastructure to provide their futures with increased usability, getting to talk with true experts in the field in different academic and social settings.

In 2019, our group focused preparing and transfer said knowledge to non-technical populations — Particularly, students of non-technical majors, participants of social movements, and human rights defenders. The students designed course materials covering the main threats to personal and group privacy, presented recommendations for behavioural changes in their online habits, and introduced the usage of several PETs — Most prominently, several Firefox extensions that allow visualizing and blocking trackers, and the use of the Tor network, via the Firefox-based Tor Browser.

The course is not limited to PETs on desktop computers; recommendations for mobile platforms were also explored, including the mobile version of the Tor Browser itself.

3 RESULTS

We show there is a clear attitudinal change on the group regarding their perceptions on security threats from privacy-invading actors. While the size of the group was too small to present statistical comparison, we can qualitatively witness the effect we had in the participants' opinions regarding protecting their data in the face of the large-scale electronic surveillance mechanisms.

4 FUTURE WORK

The course here presented is just one piece in a two year long project, along with other several deliverables. We are interested in iterating this course, both in the same faculty and to other non-technical groups. The course's curriculum will be made public in due time.

SIGCSE '20, March 11–14, 2020, Portland, OR, USA

ACM ISBN 978-1-4503-6793-6/20/03.
https://doi.org/10.1145/3328778.3372645