Training the Motivated: Digital Security for Activists

Glencora Borradaile
School of Electrical Engineering
and Computer Science
Oregon State University
Corvallis, OR 97331, USA
glencora@eecs.orst.edu

Kelsy Kretschmer
School of Public Policy
Sociology Program
Oregon State University
Corvallis, OR 97331, USA
kelsy.kretschmer@oregonstate.edu

Abstract

The state of global surveillance and the political environment has many activists caring more about their online security culture. We report on the initiation of a Digital Security for Activists program and a pilot study of an introductory seminar. Pre- and post-surveys of the seminar will form an initial assessment of what kind of intervention might increase the security practices of activists and to inform the design of program offerings. We report on the pre-surveys from three offerings of the seminar.

Introduction

In collaboration with the Civil Liberties Defense Center (CLDC), the first author had been offering informal digital security trainings for activists and their lawyers. After the fall elections in the U.S., requests for these trainings increased dramatically and shortly thereafter we launched a Digital Security for Activists (DSA) program. The DSA program's intent is to align with the CLDC mission ("to defend and uphold civil liberties through education, outreach, litigation, legal support, and assistance") and enable citizen activists to assert their constitutional rights while organizing online.

In order to provide trainings that are useful and effective, we initiated a pilot study using pre- and post-surveys of attendees of our *Introduction to Digital Security for Activists* seminar. We will use results of the survey to determine the effectiveness of the intervention (the Intro to DSA seminar) and inform a systematic design of further DSA program offerings. In this poster, we describe the Intro to DSA seminar, the purpose and goals of the accompanying pilot study, and longer range goals planned to follow the pilot. We also report initial observations after collection of the pre-survey from 57 attendees at three different training seminars. Post-survey collection of attendees at these seminars will begin in August 2017.

Intro to DSA

Trust Open-source; (warrant) canary statements; Gmail vs. Riseup [7] vs. Lavabit [11].

Authenticity of digital objects; man-in-the-middle attacks; fingerprinting.

Privacy End-to-end vs. end-to-middle encryption; meta-data; strong passphrases.

Resilience Control of digital infrastructure; reliability of communications; double-edged sword of social media.

Related Work

Many studies focus either on *average* or *expert* computer users (for example Mechanical Turkers, college students of various disciplines, security researchers), but, to our knowledge, few focus on specific user groups, such as the activist communities that attend the Intro to DSA seminar. Gaw, Felton and Fernandez-Kelly [3][1] and McGregor, Charters, Holliday and Roesner [9] report on the computer security practices of 9 employees of a non-violent direct-action organization and 15 journalists, respectively. These studies indicate that many factors contribute to the decision of whether or not to, e.g., encrypt a particular email, including usability, work flow and social pressures. While these studies paint a picture of practices for specific security-minded groups, they do not study the effectiveness of an intervention (such as training) nor do they provide guidance for best-practices with regards to interventions.

However, studies of more general populations have informed the design of the Intro to DSA seminar and pilot study. Kang, Dabbish, Fruchter and Kiesler identify four basic reasons that prevent people from adopting privacy-preserving practices: “nothing to hide”, reduced quality or convenience of tools, difficulty in using tools, and lack of knowledge in what practices to adopt [4].

Kang et al. [4] and Wash [16] identify the impact of a user’s mental model of digital communications on their perceived security risks and inclination to follow security advice. Although many studies find that more knowledge does not increase adoption of secure behaviors (e.g. [5, 14]), others find that additional motivations do result in people making more secure decisions [2, 6]. Finally, research has shown the best advice is that which is effective at addressing a problem, likely to be followed, and not too cumbersome to follow [8].

Introduction to DSA Seminar

The seminar is intended to describe elements of digital security culture that will help attendees make decisions regarding their own and their group’s digital security, as outlined in the margin. For each of the four aspects (trust, authenticity, privacy, resilience), pointers are given to specific resources, tools and technologies, for example: security-enhancing browser plugins, password managers, the Tor browser, and Enigmail with Thunderbird.

Addressing the points of the previous section, the Intro to DSA seminar starts by discussing the historical abuse of surveillance in the suppression of social movements (e.g. COINTELPRO [13]) and the current state of global surveillance [10]. Technical concepts are highlighted (e.g. how emails are transmitted, what is source code?, what are man-in-the-middle attacks) to help participants understand security risks and the reason for the advice given. Specific tools that are suggested are either easy to implement or follow-up training is offered (e.g. hands-on training for email encryption).

Depending on the time available for the training, between 5 and 15 minutes were available for questions from the

[1] Note that this paper was published in 2006, in particular, predating the global surveillance disclosures by Snowden

audience.

Concern with digital privacy		
89.5%	at least some	$5, 6, 7$
40.0%	very concerned	7

Table 1: On a scale of 1 to 7, how concerned are you about your personal digital privacy? (N = 56)

Comfort with technology		
68.0%	comfortable	> 4
17.5%	uncomfortable	< 4

Table 2: On a scale from 1 to 7, how comfortable are you using new computer programs, apps or technologies? (N = 55)

Attendee demographics	
52.6%	women
36.7%	men
52.6%	51 or older
33.3%	30 or younger
70.2%	white
8.8%	Latinx/Hispanic Chicanx

Table 3: Participants self-reported gender and ethnic identity. (N = 57)

Pilot Study Design and Goals

The object of the pilot study is an initial assessment of what kind of intervention might increase the security practices of activists. To achieve this, we seek to understand what technologies group participants are aware of to help protect their communications, as well as those they are actively using personally and in their groups. We survey attendees of the Intro to DSA seminar immediately before the seminar begins. The survey inquires as to the level of concern of the participant's privacy and the privacy of their organizing group (on a 7-point Likert scale) and their knowledge, personal and organizing use of email encryption, the Tor browser and VPNs with the option to add other privacy-preserving technologies. Participants who provide an email address will be asked to fill out the same survey again, 4-6 months following their attendance at the seminar.

From the pre-survey, we are interested in establishing a baseline for attendees knowledge and use of the technology, as well as their concern about security and comfort with new technology. From the post-survey, we will be able to assess how these elements have changed. We will also assess whether individuals take the knowledge back to their groups, that is, whether or not attendees act as vectors for transmission of information.

We also hope to inform the effectiveness of the Intro to DSA seminar as well as provide design indicators for follow-up training. For example, if individuals do act as vectors, this would support the deployment of training for trainers (as opposed to training complete groups). For participants that had access to more discussion or hands-on training, we will be able to assess the effectiveness of more in-depth training being offered at the time of the introductory seminar.

Early Observations

At the time of writing we have collected pre-surveys from 57 participants of three different Intro to DSA seminars. The first seminar was at a general training day attended by community members interested in environmental and social justice activism. The second seminar was held at the Public Interest and Environmental Law Conference and attendees included both lawyers and activists. At this conference, the CLDC, in collaboration with the first author, held a one-day drop-in center for conference attendees to access hands-on help with email encryption, mobile security and discussions of threat modeling. The third seminar was requested by a social-justice focused student group; by request of the student group, a threat modeling discussion immediately followed. The three seminars having three different types of attendees will allow for some comparison across types. We point out that by the nature of the DSA program and the CLDC through which these seminars are offered, attendees are biased left-wing politically.

From the pre-surveys and experience from the seminar, we offer the following observations. Attendees report high levels of concern about digital privacy (Table 1), which is not surprising, given that attendees had selected into a training addressing privacy and security. Comfort with new technology (Table 2) does not help us predict which respondents have knowledge of security- and privacy-enhancing technologies. Demographic measures (Table 3) also do not help predict who reports concern about security or how comfortable they are with new technology.

Participants indicate a relatively high (further comments below) use of security- or privacy-enhancing technologies (Table 4). Respondents listed 12 additional applications, with very little overlap, excepting Signal. Ten respondents added Signal to the list, with all indicating they had some

Knowledge	
TOR	31.6%
PGP	28.0%
VPN	33.0%

Use	
TOR	21.1%
PGP	17.6%
VPN	17.6%

Table 4: Participants reporting at least some knowledge and some use of TOR/TOR Browswer, PGP/GPG email encryption, and Virtual Private Newtorks (VPN).

knowledge of it, and half of them indicating they used it a great deal. Across all of these applications (including the initial three we provided), slightly more than half (51%) indicated that they had some working knowledge of a security- or privacy-enhancing technology, and 42.1% indicated they used one of the applications as least sometimes.

We also note here that that some of the applications listed by respondents were not necessarily security- or privacy-enhancing. Examples of this include Google and Whisper. This speaks to a general confusion among even people showing concern for digital security in their organizing (as has been observed by others [1]).

The category of group use is consistently lagging, with a high number of respondents leaving this question unanswered. We think this is for two different reasons. First, since so many people report little or no knowledge of the applications to begin with, it is reasonable that they simply choose to skip the question about their group's use. Second, it is possible that come attendees do not have a group or a primary group that they organize with. Of all responses, including respondents with missing data, only 19.3% of respondents report that their groups ever use any of these applications.

While the usage of PGP/GPG email encryption by attendees of the seminar is higher than one would guess of the general population, we are unaware of metrics to compare this to. However, we know that roughly 0.1% of U.S. people connect to Tor [12]. Although this percentage does not include clients connecting to Tor via a bridge and individual users may connect via multiple devices, this rate of use is far below that which we see among seminar attendees. We feel that this indicates a group of users who are willing and able to take advice regarding secure online behavior. Given the limitations of the questionnaire, it is not clear as to the purpose for participants use of VPN; however, reported use rates are double that of use across all purposes for U.S. people [15].

Questions during and at the end of the seminar are illuminating. A common point attendees raise is a variant of the "nothing to hide" [10] sentiment: that their organizing is intended to fix problems (e.g. environment, social) and that their organizing should be transparent and in the open. Attendees often want to know if what they are doing (for computer security) is enough and whether a particular application is any good.

One participant in the study, "Bob", attended two Intro to DSA seminars, filled out the survey both times, and attended additional training between the two seminars. While it is too early to measure effects of the training, we observe that Bob showed a decrease in levels of concern in regard to privacy, and indicated new knowledge and personal usage of tools, including Thunderbird and Enigmail, KeePassX, and Veracrypt (having only earlier knowledge and use of Signal). Several groups have scheduled a follow-up in-depth training that will take place before the follow-up survey.

Acknowledgements

We thank the Civil Liberties Defense Center for partnering with us and Michele Gretes and Jamil Jonna for their help in providing the Digital Security for Activists trainings. We also thank all the organizers of the specific training events.

REFERENCES

1. R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In

Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society, San Jose, CA, 137–153.

2. C. Anderson and R. Agarwal. 2010. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly* 34, 3 (September 2010), 613–643.

3. Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, New York, NY, USA, 591–600.

4. R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the Symposium on Usable Privacy and Security*. USENIX Association, Denver, CO, 39–52.

5. N. Kumar, K. Mohan, and R. Holowczak. 2008. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems* 46, 1 (December 2008), 254–264.

6. D. Lee, R. LaRose, and N. Rifon. 2008. Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology* 27, 5 (September 2008), 445–454.

7. M. Lee. 2016. Something Happened to Activist Email Provider Riseup, but It Hasn't Been Compromised. *The Intercept* (November 2016).

8. E. L. MacGeorge, B. Feng, and E. R. Thompson. 2008. *Studies in Applied Interpersonal Communication*. SAGE Publications, Thousand Oaks, CA, Chapter "Good" and "Bad" advice: How to Advise more Effectively, 145.

9. Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. 2015. Investigating the Computer Security Practices and Needs of Journalists. In *USENIX Security Symposium*. USENIX Association, Washington, DC, 399–414.

10. A. Moore. 2010. *Privacy Rights: Moral and Legal Foundations*. The Pennsylvania State University Press, University Park, PA.

11. K. Poulsen. 2013. Edward Snowden's E-Mail Provider Defied FBI Demands to Turn Over Crypto Keys, Documents Show. *Wired* (October 2013).

12. The Tor Project. 2017. Tor Metrics: Users. `https://metrics.torproject.org/userstats-relay-country.html`. (2017). Accessed May 11.

13. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Senate. 1976. *Intelligence Activities and the Rights of Americans*. U.S. Government Printing Office, Washington, DC. Report No. 94-755.

14. R. Shillair, S. R. Cotten, H.-Y. S. Tsai, S. Alhabash, R. LaRose, and N. J. Rifon. 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 48 (July 2015), 199–207.

15. T. Smith and J. Mander. 2014. *The Missing Billion: How web analytics is wiping the emerging world off the map*. Technical Report. GlobalWebIndex, London, England.

16. R. Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Symposium on Usable Privacy and Security*. USENIX Association, Redmond, WA, 1–16.