Towards an Open-Source Web Security Survey Applicable to University Students

Rafael I. Bonilla, Lenín Tenecela, Washington Vélez, Ruddy Moncayo
Escuela Superior Politécnica del Litoral, ESPOL
Campus Gustavo Galindo Km 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador
{rabonilla,lhtenece,wjvelez,rmmoncay}@espol.edu.ec

ABSTRACT

This work makes two contributions: (1) we propose the novel idea of using an open-source approach to writing surveys, and (2) we give a first step towards applying this approach in the context of surveying students about their web security literacy. Questions that interest us include: Does taking a course in security help students be more aware of the risks and vulnerabilities in their web browsing practices? When presented with a security warning, do they make the right decision? We present our results in designing and applying a survey on web security at a large university. We have released our survey instrument to the public domain and are in the process of getting other institutions to help refine the questions. We envision the following advantages of open-sourcing surveys: questions can be re-used at different institutions, results can be compared between institutions, and a world-wide community can collaborate and improve the quality of the survey instrument over time.

CCS Concepts

•**Applied computing** → **Digital libraries and archives;**

Keywords

Open-source survey; collaborative survey; security

1. INTRODUCTION

Students interact with many web-based systems in their daily life. Usually these systems are protected using various security measures. Through this use, students are sometimes prompted with messages and asked to make a security decision; for example, accept an expired digital certificate. This can happen due to benign (yet risky) reasons, such as a misconfigured server, or it can be the result of an attack (e.g., a man-in-the-middle attack). Students should decide well what action to take, as the wrong one can lead to them being denied access to a service, or can lead to a security compromise (e.g., leaked credentials). Are they really prepared to make the right choice? Do they consider all the risks? How can we measure this?

While prior work has documented the security perception of people dealing with different types of online systems (e.g., e-learning systems [2, 1]), to the best of our knowledge, there are no studies showing either the security literacy level of university students or ways to measure it. We believe it would be beneficial to evaluate students on this subject using a collaborative survey, with a set of agreed questions, so that the results (and corrective measures) can be compared and shared between institutions. To this end, we propose the novel idea[1] of using an open-source, collaborative approach, to design the survey instrument. This approach can be extended to any kind of survey whose results are of interest to multiple institutions.

We designed a web security survey applicable to students and released it to the public domain. We have applied it to 349 students at ESPOL, and are in the process of collaborating with other institutions to improve and expand the survey questions.

2. OPEN-SOURCE SECURITY SURVEYS

Using a set of well-crafted questions, we can survey students to measure their responses to various critical security scenarios.

The questions can be open-sourced and published using versioning tools (`git`), to allow a world-wide community to agree on a set of useful questions to ask students. The community could contribute adding new questions, refining existing ones and sharing their experiences with using the survey instrument. As a result, the community can a agree on the best way to assess the students and use the same questions in their evaluations. This will facilitate comparison of results and possible corrective measures.

As a first step towards a web security survey suitable for university students, we designed a set of 4 questions that test their responses when presented with a web security message. We administered the survey to 349 students from ESPOL university. 85.1% of them correctly identify the error message as an expired certificate, but just 13.75% knew the exact meaning of that; and, only 31.11% of the 45 students that were in their last semester understood the risks of accepting an expired digital certificate.

After this trial run, we improved the questions, and are in the process of applying them at other Departments in ESPOL. We have released the questions using a "Attribution 4.0 International Creative Commons" license, and have published it in Github[2]. Over time, if people find this useful, we envision a more active collaboration that will allow us to agree on a good set of questions. We are also looking for parties interested in applying the open-source approach to other types of surveys.

3. REFERENCES

[1] Costinela and Nicoleta. E-learning security vulnerabilities. *Proc. - Soc. and Behav. Sci.*, 46, 2012.

[2] Zamzuri et al. Student perception on security requirement of e-learning services. *Proc. - Soc. and Behav. Sci.*, 90, 2013.

[1]A thorough search in Google Scholar lead to no prior work on open-source surveys.

[2]In ENG and ESP: github.com/rbonillaa/Open-Source-Surveys.

ITiCSE '16 July 09-13, 2016, Arequipa, Peru

ACM ISBN 978-1-4503-4231-5/16/07.

DOI: http://dx.doi.org/10.1145/2899415.2959087