Providing an Experiential Cybersecurity Learning Experience Through Mobile Security Labs

Anthony Peruma, Samuel A. Malachowsky and Daniel E. Krutz
Department of Software Engineering
Rochester Institute of Technology
1 Lomb Memorial Drive
Rochester, NY, USA
{axp6201,samvse,dxvse}@rit.edu

ABSTRACT

The reality of today's computing landscape already suffers from a shortage of cybersecurity professionals, and this gap only expected to grow. We need to generate interest in this STEM topic early in our student's careers and provide teachers the resources they need to succeed in addressing this gap. To address this shortfall we present *Practical LAbs in Security for Mobile Applications* (PLASMA), a public set of educational security labs to enable instruction in creation of secure Android apps. These labs include example vulnerable applications, information about each vulnerability, steps for how to repair the vulnerabilities, and information about how to confirm that the vulnerability has been properly repaired. Our goal is for instructors to use these activities in their mobile, security, and general computing courses ranging from secondary school to university settings. Another goal of this project is to foster interest in security and computing through demonstrating its importance. Initial feedback demonstrates the labs' positive effects in enhancing student interest in cybersecurity and acclaim from instructors. All project activities may be found on the project website: http://www.TeachingMobileSecurity.com

CCS CONCEPTS

• **Social and professional topics** → **Software engineering education**; • **Security and privacy** → *Software security engineering*; *Domain-specific security and privacy architectures*;

KEYWORDS

Security Education, Security Labs, Mobile Education

ACM Reference Format:
Anthony Peruma, Samuel A. Malachowsky and Daniel E. Krutz. 2018. Providing an Experiential Cybersecurity Learning Experience Through Mobile Security Labs. In *SEAD'18: SEAD'18:IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment , May 27, 2018, Gothenburg, Sweden.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3194707.3194712

SEAD'18, May 27, 2018, Gothenburg, Sweden

ACM ISBN 978-1-4503-5727-2/18/05…$15.00
https://doi.org/10.1145/3194707.3194712

1 INTRODUCTION

Most would agree that mobile devices have changed the way we live, work, and communicate. While mobile apps offer an unprecedented view into our daily lives, cybersecurity in mobile app development, unfortunately, continues to largely be an afterthought. As an example, one of the leading Android development books on Amazon [12] has only has 17 of its 671 pages devoted to security, only addresses encryption, and is contained within the very last chapter of the book. This terse and secondary consideration to mobile security unfortunately represents the norm when it comes to security education [2].

To address this challenge, we created the *Practical LAbs in Security for Mobile Applications* (PLASMA) project [16], which contains eleven labs devoted to mobile security education. Each lab addresses a different mobile security principle such as secure data storage, intent protection, and proper use of external libraries. Each lab contains I) Background on the vulnerability II) A sample app containing the vulnerability III) Steps to recreate the vulnerability, and IV) A demonstration of vulnerability removal. The PLASMA labs have already been presented several outreach events, at conferences such as NYCWIC [6], at the SEED Security workshop [11], and even abroad at the Technical University of Berlin [5]; receiving positive feedback at these events. The objective of the labs is to not only teach about a specific mobile vulnerability, but to importantly create interest in mobile security for those students. The PLASMA labs were in part created to address the lack of labs exclusively devoted to mobile app security.

Experiential learning has been shown to be beneficial to computing education [10, 15, 17] and is comprised of four primary stages: abstract conceptualization, active experimentation, concrete experience, and reflective observation [9]. Experiential learning provides a complete learning experience for the student, one where they both understand the concept behind an idea and interactively learn through doing. The two aspects of this cycle which are especially important to teaching are the emphasis on subjective and concrete experiences for the student and the translation of concepts through observation and reflection [18]. To provide a robust educational environment, it is imperative to create activities where students are not only instructed in a topic, but where they are able to actively experience it as well [14].

1.1 Project Objectives

Creating accurate, robust security activities can be a difficult and time consuming task for instructors; our goal is assisting instruction in mobile, security, and general computing courses. Additionally, these labs have already shown value in computing outreach events [5, 6]. Each lab has been systematically designed to meet the intended educational objectives and to make adoption as easy as possible. Other than the freely available Android Studio IDE, no special software is required. Instructors may choose to adopt as many labs for their class or event as they would like, as they are intended to be used in an à la carte fashion.

The design of the labs are guided by two objectives, which are based on our belief in two teaching philosophies:

Philosophy 1: *Mobile security education should provide real-world examples. Students should be provided opportunities to learn from real-world situations that provide an appropriate background, context, and relevance for the examples.*

Software security is a diverse field and includes topics ranging from social engineering to cryptography and can be covered in a variety of courses and situations from general programming to advanced security courses. Regardless of the course and topic, for students to learn to properly protect themselves from a vulnerability they must I) Understand why the vulnerability is detrimental, II) Understand the cause of the vulnerability, and III) Understand how to repair/protect against the vulnerability. We have created labs that fulfill these criteria. These principles shape the first objective of this project: *to provide labs which cover a wide range of mobile security principles based on real-word examples.*

Philosophy 2: *Software security is important to everyone and software security education should be available to everyone.*

All computing students need to learn about security. Even minor vulnerabilities in the design or implementation of an application can have profound effects on all project stakeholders. Students should not be inhibited from learning about software security due to institution or instructor constraints. Since software security may be included in a diverse set of courses and situations, instructors should be able to pick and choose relevant materials and activities in an à la carte fashion. These adaptable labs enable instructors to select the most relevant materials for their courses from utilizing a single lab to basing their entire course around our provided materials. These principles shape the second objective of this project: *to provide high quality, self-contained labs which are ready to be used in a variety of settings and contain all related instructional and activity materials.*

2 RELATED WORKS

The SEED security labs [11] have achieved considerable world-wide success have been adopted at over 600 schools on six continents. These labs cover diverse topics including attacks, software security, system security, network security, vulnerabilities, web security, and cryptography. Our project differs in that SEED only has two labs devoted to mobile system security, which differs from the application security focus of our project.

There are many existing security exercises which may be found from a variety of sources including online blogs and funded NSF grants. Although there are a plethora of online resources for teaching various security principles [1, 4, 7, 8], these resources are deficient in a variety of ways, including: I) they may not have been examined by security experts to ensure their quality, II) they are not created in a uniform fashion (each activity is often conducted in an inconsistent manner) III) they do not contain a diverse set of security related activities, and IV) they do not contain supplementary educational materials. While very beneficial, the CyberPaths [3] security labs do not focus on mobile security. While the Cyberpaths labs, SEED labs, and other similar projects differ from our PLASMA labs, they serve to demonstrate the capabilities and impact of easily adoptable mobile security activities such as our PLASMA labs.

3 PLASMA LABS

We will next provide an overview of the lab components, a list of current labs, and a brief example of an existing sample lab.

3.1 Lab Components

While we are continually developing new labs, there are currently eleven vulnerability labs ranging from *proper intent protection* to more complicated activities such as *correct use of content providers*. Our objective is to create labs that not only inform students about how to create secure software, but also to motivate students to create secure software. We've created an experiential learning environment where the students directly witness the effects of the vulnerability and then are able to repair it. Each of the exercises contain:

(1) Example Mobile apps with well defined vulnerabilities
(2) Documentation on the adverse effects of the vulnerabilities and how they may be exploited
(3) Step-by-step instructions in repairing the vulnerable app
(4) Instructions on how to verify that the vulnerability has been repaired
(5) Examples of the apps which have already have had the vulnerabilities repaired

Activities provide background (when, why, and how the vulnerability may occur) about the specific vulnerability being targeted, and, whenever possible, users are also provided with a real-world example of occurrences of the vulnerability. Also included are some basic reasons why the vulnerability occurs and common developer mistakes which lead to the vulnerability.

3.2 Current Labs

There are eleven security labs in our educational set, although this number will grow as new labs are developed.

(1) **Activities Access:** Security issues arise when people try to access unauthorized activities. An example is a bank app where users try to access a balance management activity without logging into the system.
(2) **Intent Protection:** Android uses "Intents" to pass data between apps, for examples between the Facebook and Facebook Messenger apps. Data passing between these apps may be easily (and improperly) read by other apps. This lab explains how to protect information being sent via Intents between apps.

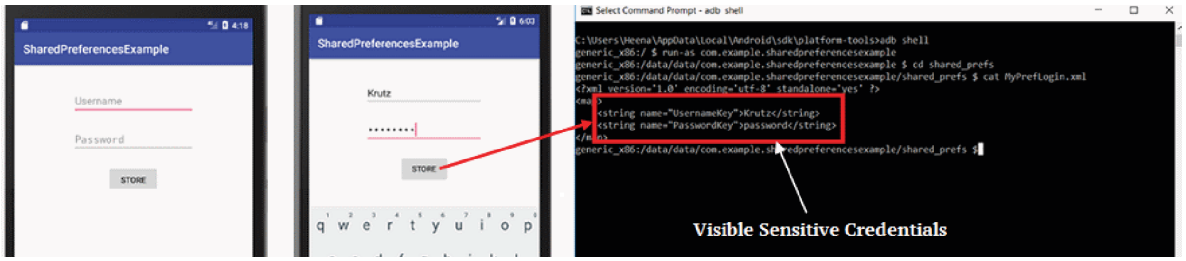

Figure 1: Example PLASMA Lab Showing Effects of Insecure Software

(3) **XML Protection:** XML is easy to read using reverse engineering, so it is best to avoid saving important information like Ads Code or Map Code within XML files.
(4) **Android Javascript:** This demonstrates the negative implications of using JavaScript in Webview to pass data from an Android app to a server. This is considered bad practice because anyone could use malicious JavaScript code on their website to gain private user information associated with the app.
(5) **Broadcast:** Broadcast data sent by the app is easy to access from any other app in the system, so when Broadcasting to specific apps, the data should be encrypted. Intercepted unencrypted Broadcasts could lead to serious security and privacy issues.
(6) **Data Storage:** When an app does not secure storage data like data files, shared references, and databases (i.e. SQLite), it has the potential to be read by any other app. This means that important information stored in these files (such as database connection information) should be encrypted.
(7) **DataOverHTTP:** Data that moves over an unencrypted HTTP (Internet) connection is vulnerable to "man in the middle" attacks. One example of this is credit card information, which, if passed over an unsecured connection, could be intercepted midstream.
(8) **DoS:** Denial of Service (DoS) attacks are a common problem with Android, because a malicious party could create an overwhelming number of HTTP requests directed towards a specific server. Environments must be managed to make them less vulnerable to these types of attacks.
(9) **Services:** Services, particularly bound services, can be accessed by any app on a device if not properly protected. There must always be one or more ways of keeping a service secure and accessible only to trusted apps.
(10) **AdLibrary Usage** Using Ad libraries can open up various security and privacy issues within the app including sensitive user information such as location or contact info.
(11) **Content_Providers:** Content providers share data between apps. Due to this, data stored here must be kept secure and encrypted so that it can only be read by an authorized app.

4 PRELIMINARY RESULTS

Although we have yet to conduct a thorough analysis of the educational labs, initial results indicate the benefits of the labs for both students and instructors. The results described below are not intended to be a definitive evaluation of the effectiveness of the labs, but merely serve to indicate the initial results in demonstrating their effectiveness. All studies were approved by the relevant institutional review board (IRB).

4.1 Student Survey

The labs have been used in several student outreach events [13] for local High School Students, university student groups, and even internationally at TU-Berlin [5]. Before and after participating in the lab activities, students were asked to complete an anonymous survey. A total of 55 participants completed both surveys.

Motivating students to pursue the area of cybersecurity should be an important goal for any cybersecurity educational project. We asked participants the question "How interesting do you view the topic of software security?". The results of this survey before and after the students completed two labs in an outreach event are shown in Figure 2. We also asked students "How interested are you in taking a security-related course in the future?". The results of this survey are shown in Figure 3.

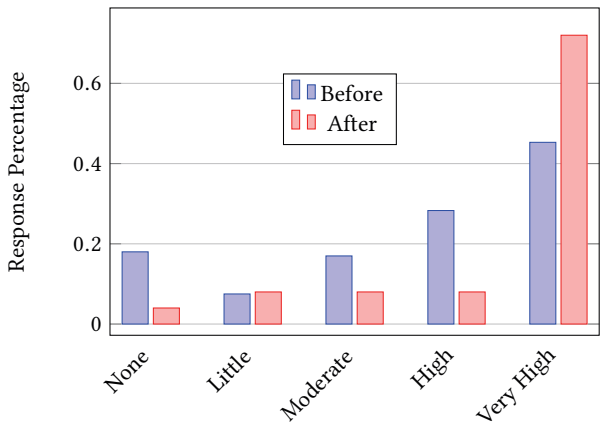

Figure 2: General Student Interest In Security Before and After Labs

The results in Figure 2 demonstrate the effectiveness of the labs in growing student interest in security. Figure 3 indicates that some students who only had a 'Moderate' amount of interest in taking a cybersecurity course prior to using the labs switched to having a 'High' interest after using the labs. Although these results are preliminary, they indicate that the labs are an effective tool in motivating students on on the topic of cybersecurity.

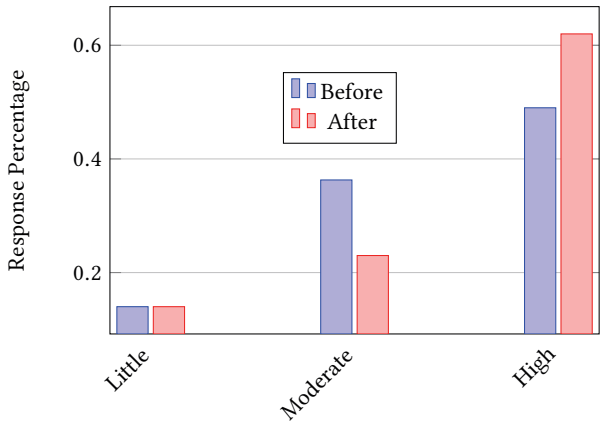

Figure 3: Student Interest In Taking a Cybersecurity Course Before and After Labs

In the post-lab activity survey we also asked students to provide further anonymous feedback on the labs. Table 1 shows the results for the likert question *How much did you learn from the activity.* Table 2 shows the responses for the questions *Would you recommend this activity to a friend who wants to learn about security?* and *Do you feel like the activity resembles a security issue which could occur in the real world?*. These results are an initial indication of the effectiveness of the lab.

Table 1: How Much Student Learned

Question	Little	Moderate	A Lot
How much did you learn?	.03	.53	.44

Table 2: Student Feedback

Question	No	Yes
Recommend to Friend	.06	.94
Resemble Real-World	.10	.90

4.2 Instructor Feedback

We conducted two workshops in the summer of 2017 for both U.S. and international college instructors. At the conclusion of the workshop, we used an anonymous survey to ask instructors how likely they would be to use the activities in their classes and outreach events. The results are shown in Table 3. A total of 49 instructors completed the survey at our workshops.

Table 3: Likelihood of Instructor Lab Adoption

Question	Unlikely	Somewhat	Very
Adoption Likelihood	.06	.23	.71

5 FUTURE WORK

We will continue to build upon our created labs by:

(1) Creating new labs, including iOS activities
(2) The inclusion of teaching materials including instructor slides, quizzes, and instructional videos
(3) Continuing to evaluate the educational effectiveness of the labs. This includes the ability to both inform and motivate students about creating secure software
(4) Creating a single Virtual Machine for ease of adoption
(5) Continued use in outreach events

6 CONCLUSION

We present eleven publicly accessible mobile security educational labs that can be adopted in a variety of educational settings including classrooms and outreach events. The labs have been systematically designed to cover a wide range of mobile security principles and have already demonstrated their educational effectiveness in motivating student interest in cybersecurity.

ACKNOWLEDGEMENTS

Elements of this work are sponsored by a SIGSCE Grant.

REFERENCES

[1] Android secure coding standard. securecoding.cert.org/ confluence/pages/viewpage.action?pageId=111509535.
[2] Cloudpassage study finds u.s. universities failing in cybersecurity education. https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/.
[3] Collaborative project: Engaged student learning: Design and development, level i: Broadening the path to the stem profession through cybersecurity learning. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1700254&HistoricalAwards=false.
[4] Exploitme mobile android labs. securitycompass.github.io /Android-Labs/setup.html.
[5] Mobile security workshop: Tu-berlin. http://tub.teachingmobilesecurity.com.
[6] Nycwic 2017. http://nycwic.hosting.acm.org/.
[7] Owasp mobile security project. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Home.
[8] Tutorial: Build an android application with secure user authentication. https://stormpath.com/blog/build-user-authentication-for-android-app.
[9] D. Boud, R. Keogh, and D. Walker. *Reflection: Turning experience into learning*. Routledge, 2013.
[10] C. Brown, R. Pastel, M. Seigel, C. Wallace, and L. Ott. Adding unit test experience to a usability centered project course. In *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, SIGCSE '14, pages 259–264, New York, NY, USA, 2014. ACM.
[11] W. Du. Seed labs. http://www.cis.syr.edu/ wedu/seed/.
[12] H. Franceschi. *Android App Development*. Jones & Bartlett Learning, 2016.
[13] Hidden. http://www.xxxxx.
[14] C. E. Irvine et al. Amplifying security education in the laboratory. 1999.
[15] S. Krusche, A. Seitz, J. Börstler, and B. Bruegge. Interactive learning: Increasing student participation through shorter exercise cycles. In *Proceedings of the Nineteenth Australasian Computing Education Conference*, ACE '17, pages 17–26, New York, NY, USA, 2017. ACM.
[16] D. Krutz. Plasma labs: Teaching mobile security. http://www.TeachingMobileSecurity.com/.
[17] L. Laird and Y. Yang. Engaging software estimation education using legos: A case study. In *Proceedings of the 38th International Conference on Software Engineering Companion*, ICSE '16, pages 511–517, New York, NY, USA, 2016. ACM.
[18] K. Shaw and J. Dermoudy. Engendering an empathy for software engineering. In *Proceedings of the 7th Australasian Conference on Computing Education - Volume 42*, ACE '05, pages 135–144, Darlinghurst, Australia, Australia, 2005. Australian Computer Society, Inc.