The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #43440

Exploring Cybersecurity Hands-on Labs in Pervasive Computing: Design, Assessment, and Reflection

Prof. Anyi Liu, Oakland University

Anyi Liu received his Ph.D. degree in Information Technology from George Mason University, Virginia. He is currently an Associate Professor in the Department of Computer Science and Engineering at Oakland University, Michigan, USA. His research interests primarily lie at the intersection of system security, software security, intrusion detection, intrusion prevention, and digital forensics. His research is supported by the National Science Foundation and Michigan Space Grant Consortium. He is a Senior Member of the IEEE.

Dr. Bruce R Maxim, University of Michigan, Dearborn

Bruce R. Maxim has worked as a software engineer, project manager, professor, author, and consultant for more than forty years. His research interests include software engineering, human computer interaction, game design, virtual reality, AI

Xiaohong Yuan, North Carolina A&T State University

Dr. Yuan is a professor in the Department of Computer Science at NCA&T. Her research interests include AI and machine learning, anomaly detection, software security, cyber identity, and cyber security education. Her research has been funded by the National Security Agency, the National Centers of Academic Excellence in Cybersecurity (NCAE-C), the National Science Foundation, the Department of Energy, the Department of Education, etc. She has served on the editorial board for several journals on cybersecurity.

Dr. Yuan Cheng, Grand Valley State University

Dr. Yuan Cheng is currently an associate professor in the School of Computing at Grand Valley State University. Previously, he held a tenured faculty position in the Department of Computer Science at California State University, Sacramento. He earned his Ph.D. in Computer Science from the University of Texas at San Antonio. His educational background also includes a B.Eng. degree in Information Security from Huazhong University of Science and Technology, Wuhan, China. His research interests include access control, authentication, Internet of Things, privacy, and social computing.

Exploring Cybersecurity Hands-on Labs in Pervasive Computing: Design, Assessment, and Reflection

Abstract

The increasing demand for versatile and mobile computing has made pervasive computing a crucial component of the high-performance, low-cost computing paradigm for research and education. While existing efforts have developed cybersecurity curricula, platforms, and hands-on labs for cloud, mobile, and cyber-physical systems (CPS), the core properties of pervasive computing remain insufficiently covered. This paper addresses these challenges by comprehensively covering security and privacy in pervasive computing. We develop curricula and hands-on labs that systematically address the essential properties of pervasive computing. Rather than simply combining materials from previous efforts, we compare existing cybersecurity education work and explore intrinsic connections, overlaps, and combinations. Our curricula aim to provide students with a thorough understanding of security and privacy in pervasive computing. We then present the ReScuE, a free and cloud-based cyber range that is scalable, safe, easy to set up and maintain, and facilitates high privileges for educators to oversee students' hands-on practice progress. To facilitate widespread adoption, we developed a set of virtual-machine- and container-based hands-on labs on top of the ReScuE, covering various disciplines of pervasive computing for different educational purposes. Each lab includes progressive hands-on practices, defined knowledge units, and learning outcomes based on the CSEC 2017 Curricular Guidelines, ensuring consistent quality and broader adoption. After iterative development and multiple pilot assessments, we conducted formal evaluations from 2018 to 2022 at two institutions. We define research questions for our pedagogic research through continuous refinement with student feedback. Our study demonstrates that the ReScuE labs received high satisfaction ratings from students with diverse ethnic and academic backgrounds before and during the COVID-19 lock-downs. The comprehensive coverage of pervasive computing cybersecurity allows students to learn state-of-the-art research findings, gain hands-on experiences with recent software, and engage with cutting-edge cybersecurity technology. Finally, we share the lessons we learned from our study, make ReScuE lab materials available to the public, and aim to benefit the broader audience of cybersecurity education.

1 Introduction

As a growing computing paradigm, pervasive computing allows devices to interconnect and understand their surroundings with minimal human intervention. With the empowerment of high-performance cloud infrastructure and low-cost network connectivity, pervasive computing can perform collaborative jobs by collecting and analyzing data and communicating among mobile devices and sensors. However, the increasing attention to pervasive computing introduces new security issues and challenges. Thus, equipping students with the knowledge and skills to handle the security issues of pervasive computing is crucial yet challenging for educators.

Prior efforts have shown initial success in training students with hands-on cybersecurity labs focusing on cloud and mobile computing. However, some fundamental knowledge areas (KAs) and knowledge units (KUs) have not been adequately studied. While significant effort has been invested in constructing cloud-based infrastructures or testbeds[1,2,3,4], network security labs[5,6], and mobile security labs[7], educational materials related to specific topics of pervasive computing are still scarce. For example, new cryptosystems, new exploits at the application level, and new techniques that nourish students' analytical mindset in digital forensics are missing in the prior literature. Moreover, although most existing works engage students and examine their feedback, little research continuously studies students' feedback and uses it to improve the quality of their materials in the long run. An adequate solution to these issues is required for the broader adoption of cybersecurity curricula.

In this paper, we present ReScuE, a cloud-based framework coupled with a suite of hands-on labs in various disciplines of pervasive computing, including new cryptosystems, new offensive technology in mobile computing, and new defensive and analytic technology in mobile computing and digital forensics[1]. The ReScuE framework is highly scalable, and its labs cover different security and privacy facets of pervasive computing, which makes it versatile for various educational purposes. Between 2017 and 2022, we performed pilot studies, formal assessments, and continuous refinement at two institutions. The assessment results show that the ReScuE labs achieve a high satisfaction rate and positive learning experiences regardless of students' ethnic and academic backgrounds. Similar results were observed even during the COVID-19 pandemic when we transitioned to online teaching and learning.

2 Related Work

The rise of virtualization and cloud computing has enabled cybersecurity educators to efficiently teach students by utilizing public cloud platforms like CloudLab[1] and GENI[4], as well as commercial cloud services such as AWS[8] and Azure[9]. Researchers like Park et al.[5] and Mountrouidou et al.[10] have designed lab modules on CloudLab and GENI, respectively, to enhance students' learning and research interests in SDN. These lab modules incorporate state-of-the-art network security technologies from their research, making it easy for students to understand and replicate. In addition, EDURange[6], developed by Weiss et al., creates an interactive environment for teaching network and operating system labs, while Khaled et al. use Amazon AWS to teach computer networks[11,12]. Most existing work leverages the cloud to create a virtual lab environment for teaching offensive or defensive technology and tools at the *network layer*. One example is the SEED labs[13] developed by Du et al., which covers a wide range of cybersecurity topics and focuses on fundamental knowledge of computer systems, software, and networks. In contrast, the ReScuE labs concentrate on teaching offensive or defensive technology and tools at the *application layer*, covering topics such as mobile security, forensics, and cryptography. As a result, the ReScuE labs offer distinct benefits that complement previous efforts.

[1] ReScuE, A Hands-on Labs Suite for Pervasive Computing. https://github.com/anyiliu-mi/ReScuE

Infrastructure as Code (IaC) language[14] is gaining popularity among researchers as it helps to overcome the technical challenges of creating scalable lab environments in the cloud. For example, Cyber Range Instantiation Systems (CyRIS)[15] and KYPO[16] use YAML specification to deploy software and create cloned virtual instances for students, while CRACK[17] and Austrian Institute of Technology (AIT)[18] use higher-level scenario-definition language (SDL) on top of an IaC specification to configure OpenStack cloud infrastructure. Yamin and Katt[19] also use SDL to simulate vulnerabilities, attacks, and defensive actions in their educational cybersecurity environment. Furthermore, CyberArena[20], an open-source cloud-based platform, uses IaC to build various cybersecurity labs, making cybersecurity education accessible to a broader audience while reducing technical barriers and costs.

Table 1: Comparing the ReScuE with other cybersecurity educational projects.

Projects	Primary objectives	Key features	Features to be desired
CloudLab	Cloud-based platform for research and education	General-purposed and free	Supporting cybersecurity education
AWS and Azure	Cloud-based platform for business	Reliable and not free	Supporting cybersecurity education
SDNLab	Conveying SDN/NFV research to education	Technical and domain-specific	Including domains beyond SDN/NFV
GENILab	Leveraging GENI for cybersecurity education	Flexible and easy to use	Sticking hands-on exercises to GENI
EDURange	Training student's analysis skills	Flexible and easy to use	Desiring recent technology
SEED	Covering cybersecurity fundamentals systematically	Comprehensive and technologically advanced	Providing various levels for non-R1 universities
CyRIS	Defining and deploying virtual instances for learners	Focusing on building the system	
KYPO	Building cyber-competition scenarios	Orchestrating the low-level infrastructure	No emphasis on pervasive computing
CRACK	Defining higher-level cybersecurity scenarios	Easy to use	Not focus on pervasive computing
AIT	Using higher-level language to specify and deploy cybersecurity scenarios	Easy to use	Not focus on pervasive computing
CyberArena	Constructing scalable cybersecurity labs	Open-source	Lacking explicit scaffolding tasks
ReScuE	Constructing free cloud-based platforms	Easy to use and scalable	Designing more labs

Table 1 compares the ReScuE with other cybersecurity educational projects. It is important to note that these projects were built with different goals and times. We intend not to criticize them but to highlight their primary objectives and features to differentiate them from the ReScuE. We focus on developing students' cybersecurity skills in various sub-domains of pervasive computing by creating free cloud-based platforms. Although we currently use CloudLab, our implementation can be deployed on any platform that supports the OpenStack cloud infrastructure[21].

Our evaluation of students' feedback also responds to Švábenský et al.[22], which addresses some common issues in existing publications on cybersecurity education. Our research collected feedback from 287 students over five years (2018-2022) to answer these common issues, a much larger sample size. Finally, we ensure the quality and broader use of the ReScuE labs by following the

CSEC 2017 Curricular Guidelines[23], which define the knowledge units and learning outcomes of each lab, making it easier for educators to select the appropriate ones for their objectives.

3 The ReScuE Platform and Labs

3.1 System Overview

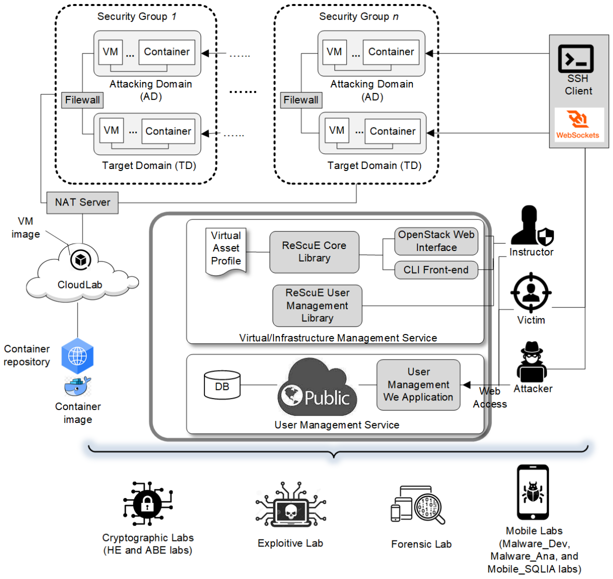


Figure 1: The system architecture of the ReScuE platform.

The ReScuE framework has two components: 1) a *cloud-based platform* and 2) a series of *course modules* and *hands-on labs*. As illustrated in Figure 1, the platform is built upon CloudLab[5] that facilitates virtual artifacts, such as networks, VMs, and containers. It comprises two services: 1) Virtual/Infrastructure Management Service (VMS) that supports key functionalities of constructing, managing, backing up, and restoring virtual artifacts, and 2) User Management Service (UMS) that obtains the information about virtual artifacts from CloudLab and then assigns them to students upon requests. Instructors can monitor the usage of virtual artifacts through a command line interface (CLI) and web interfaces of CloudLab and ReScuE. Once the virtual environment is constructed, students can access virtual artifacts via an SSH client or web socket terminal and play as the victim, attacker, or both. A pilot study on the ReScuE platform was published in 2018[24].

Course modules and hands-on labs account for the other essential components of the ReScuE framework. We design six hands-on labs that cover different aspects of pervasive computing, with a particular focus on cloud-based exploit and forensics (*Cloud exploit & forensic lab*), cryptography for privacy-preserving (*HE lab*) and access control (*ABE lab*), and mobile computing (*Malware_Dev*, *Malware_Ana*, and *Malware_SQLIA labs*). For each lab, we clearly describe learning objectives and expected outcomes in the manual. There are three levels of tasks: 1) the *Follow-me level*, 2) the *DIY level*, and 3) the *Trophy level*. The benefits of defining three levels of tasks are apparent. First, it progressively scaffolds students' understanding and ensures students complete a lab within a reasonable duration. Second, we can easily customize tasks at different educational

Table 2: The suggested pervasive adoption schemes.

Levels	Target Audiences	Materials
Follow-me	K-12, out-reach, and gen-ed.	pre-lab lecture notes, demo videos, lab manuals, brainstorming discussions, and post-lab surveys.
DIY	2-yr and 4-yr college students (1st- and 2nd-year).	
Trophy	4-yr college student (3rd- and 4th-year) and graduate students.	

levels for pervasive adoption. Table 2 lists our suggested adoption schemes for students at different levels.

3.2 Hands-on Labs Design

Next, we present the detailed design of the ReScuE labs. In addition, we map KAs and KUs proposed by the Joint Task Force (JTF) on Cybersecurity Education[23] to each lab and allow the cybersecurity education community to choose the appropriate lab modules for their needs.

3.2.1 Cloud-based malware construction and virtual machine forensics (*Cloud exploit & forensics lab*)

This lab helps students gain knowledge of malware construction with Metasploit[25] for both Ubuntu VM and Android. Students should accomplish the hands-on lab tasks that include: Constructing exploits; probing the vulnerabilities of VM through virtual machine introspection (VMI) and Android network penetration tool; launching exploits to gain remote access to the victim's machine. After running a successful exploit, students should write programs with VMI API to retrieve the digital artifacts from the VM and analyze the network traffic.

Learning Outcomes Upon completion of the lab, students will be able to use OpenVAS[26] to discover system and software vulnerabilities; use Metasploit Framework (MSF)[27] to construct exploits; and get familiar with Volatility[28] VMI API for conducting a forensic analysis on the compromised machine.

KA: KU Data: Forensics, Component: Vulnerabilities,
System: Thinking, System: Control, and Organizational: Risk.

3.2.2 Fine-grained Access Control with Attribute-based Encryption (*ABE Lab*)

This lab helps students better understand attribute-based access control (ABAC) and Attribute-based Encryption (ABE). First, the instructor introduces two different ABE techniques, Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE), and their applications. Then, the instructor gives students freeware that supports CP-ABE[29] and KP-ABE[30]. The lab tasks include: composing the security policies according to various realistic scenarios, integrating security policies into crypto-keys; and decrypting messages using the correct crypto-keys.

Learning Outcomes Upon completion of the lab, students will be able to describe attribute-based encryption, compose security policies per different needs; integrate security policies into crypto-keys, and decrypt ciphertexts using correct crypto-keys.

KA: KU Data: Cryptography, Data: Access Control, and Human: Identity.

3.2.3 Processing encrypted data with Homomorphic Encryption (*HE Lab*)

This lab helps students build a solid understanding of the purpose of HE and the confidentiality issues in a supply chain. In particular, students should learn the following: Understanding basic cryptographic operations (addition, subtraction, multiplication, etc.) that HE supports; using these cryptographic operations to write applications at the program level; solving real-world problems by utilizing HE. Of course, we provide both the HE library and APIs to students.

Learning Outcomes Upon completion of the lab, students can use HE cryptographic operations at the command-line and program level; and solve real-world problems with the HE cryptosystem.

KA: KU Data: Privacy, Component: Procurement, and Human: Usable Security and Privacy.

3.2.4 Developing Mobile Malware (*Malware_Dev Lab*)

This lab walks through the process of developing a piece of mobile malware from scratch. Students should learn how to 1) design and develop a piece of malware that sends text messages to all the contact list of the user's device, 2) design and develop a Trojan horse program that steals a user's sensitive information and sends it to a remote server, and 3) run Metasploit's "`exploit/android/*`" module to create various exploits.

Learning Outcomes Upon completion of the lab, students should be able to get familiar with the Android Debug Bridge (adb); run Metasploit's "`exploit/android/*`" module to create exploits; develop malware that sends text messages from the victim; and develop malware that steals a victim's sensitive data.

KA: KU Software: Design, Software: Implementation, and Social: Cybercrime.

3.2.5 Behavior-based Mobile Malware Analysis and Detection (*Malware_Ana Lab*)

In this lab, students should learn how to use program analysis tools to analyze the apps and report malicious activities/behaviors. The analysis can be done statically (at the source or byte-code level) or dynamically (while the app runs). Instructors should introduce some existing program analysis tools to students.

Learning Outcomes Upon completion of the lab, students should be able to use FlowDroid[31] and MobSF[32] to perform static analysis against malware; and use VirusTotal[33] to perform dynamic analysis against malware.

KA: KU Data: Forensics; Software: Analysis and Testing, and Organizational: Analytical Tools.

Table 3: The attributes for the characters in '*Harry Potter and the Philosopher's Stone*".

Users List			
User Name	DOB	Hair Color	Level
Harry Potter	July 31, 1980	Black	Student
Ron Weasley	March 1, 1980	Blond	Student
Quirinus Quirrell	September 26, 1970	Black	Professor

3.2.6 Apps SQL Injection and Defense (*Mobile_SQLIA Lab*)

This lab helps students understand how SQLite databases work in apps and how SQL injection attacks execute on a mobile device. In particular, students design and create a simple SQL injection attack that leverages the SQLite Databases of Android. As a result, students understand the security vulnerabilities in a database and mobile applications.

Learning Outcomes Upon completion of the lab, students can design and create a simple but vulnerable application that leverages the SQLite Databases of Android; and explains the security vulnerabilities in a database and mobile applications.

KA: KU Software: Implementation and System: Thinking.

4 Sample Labs

This section briefly describes two mini-modules of ReScuE labs: 1) Ciphertext-Policy Attribute-based encryption (CP-ABE) and 2) Mobile Malware Development. The process of conducting each lab will be elaborated on in the next section.

Ciphertext-Policy Attribute-based encryption (CP-ABE) Lab The CP-ABE lab starts with the narrative of the learning objectives and background knowledge. Then, we give students the instructions and commands for downloading Docker containers. Finally, as the first case study, we provide a simple example with all required Linux commands to generate user keys according to their attributes and encrypt data with a specific access control policy. After that, we provide another set of Linux commands that decrypt ciphertext with the users' key. As a result, we show that only the user whose attributes satisfy with access control policy will decipher the ciphertext. Now, we compose the following scenario of "*Harry Potter and the Philosopher's Stone*" and ask them to practice the CP-ABE.

Let's assume three characters' attributes are specified in Table 3, whose information came from Wikipedia[34]. A confidential document is now encrypted by Hermione Granger, whose content is only viewable by Harry Potter and Ron Weasley. In other words, only Harry and Ron can decrypt and read the document, while Professor Quirrell cannot. You should create a random document for your own and demonstrate this scenario.

This lab task assumes that a confidential document is encrypted by Hermione Granger, whose content is only viewable by Harry Potter and Ron Weasley. In other words, only Harry and Ron can decrypt and read the document, while Professor Quirrell cannot. Students should demonstrate this scenario with two deliverables:

1. *Let's say you are Hermione Granger. Please provide command lines that encrypt the document. Also, please include the screenshot(s) to demonstrate that the document has been encrypted successfully.*

2. *Please provide command lines that show Harry Potter and Ron Weasley can decrypt the ciphertext. Also, provide the command line(s) that shows Professor Quirrell cannot decrypt the ciphertext or ends up with failure.*

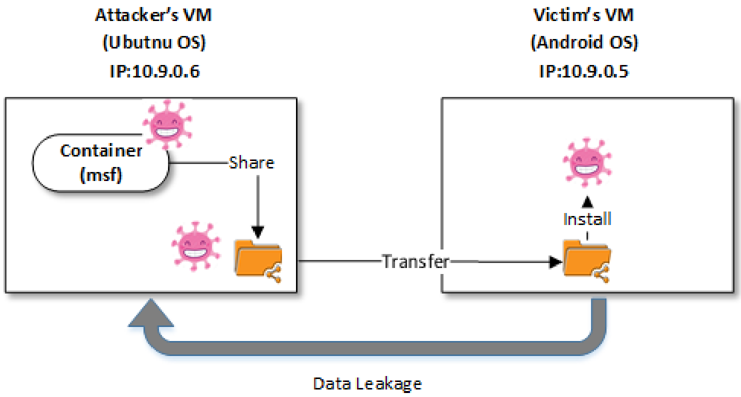
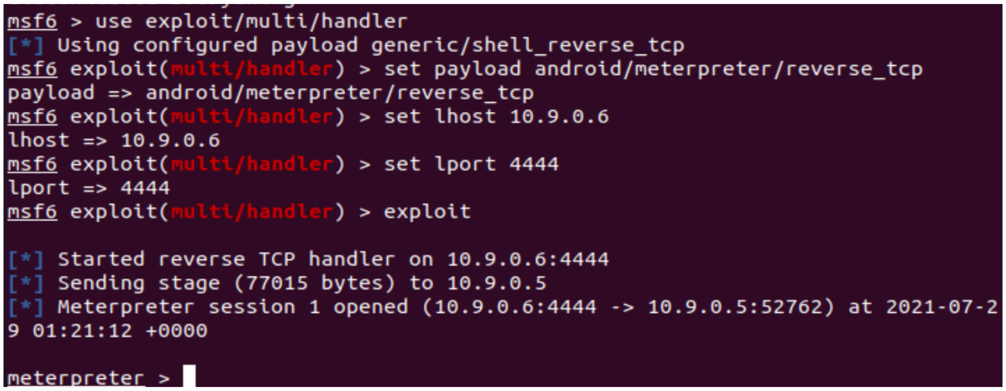


Figure 2: The attacking scenario includes two VMs and one container.

Mobile Malware Development For this lab, students are asked to develop a mobile malware from scratch or by using Metasploit Framework (MSF)[25]. The attacking scenario is illustrated in Figure 2. In the scenario, students were first asked to start two VMs (the attacker's and the victim's VMs). Then, inside the attacker's VM, pull a container pre-installed with the MSF console. Using the MSF console to construct the mobile malware and share it with the attacker's VM. After that, install the mobile malware on the victim's VM and launch the exploit. Finally, students should be able to control the victim from the attack's VM. For this lab module, students should work with two deliverables:

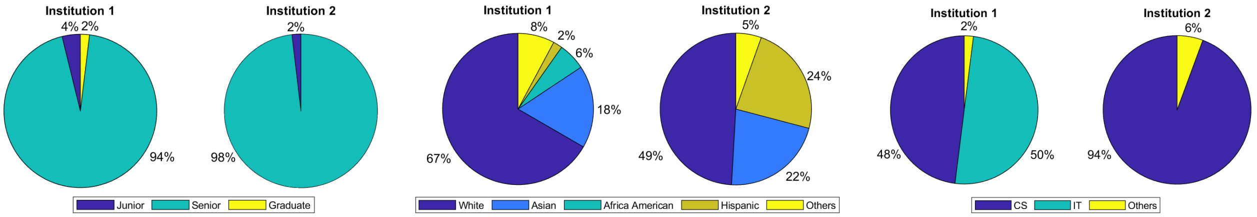


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.9.0.6
lhost => 10.9.0.6
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.9.0.6:4444
[*] Sending stage (77015 bytes) to 10.9.0.5
[*] Meterpreter session 1 opened (10.9.0.6:4444 -> 10.9.0.5:52762) at 2021-07-2
9 01:21:12 +0000

meterpreter >
```

Figure 3: Session information output on the attacker's VM.

1. *In the* `meterpreter` *console, run MSF commands to control the victim VM. You should be able to see a screenshot similar to the one in Figure 3.*
2. *Explain why the exploit can be launched successfully.*

5 Evaluation Setup



(a) Student Classification (b) Ethnicity (c) Majors

Figure 4: Students' ethnic and academic background at Institutions 1 and 2.

5.1 Lab and Assessment Setup

The lab tasks are conducted in a physical classroom or online, following a standard process. Most students were unfamiliar with or had not used the particular toolchain before. Figure 5 illustrates the process of conveying knowledge with hands-on labs. First, the instructor lectures cybersecurity fundamentals by embedding our course modules. The instructor also introduces the toolchain and demonstrates examples that enhance students' comprehension. Then, the instructor asks students relevant questions about the knowledge units and collects their answers. The instructor then plays recorded videos, articulates hands-on tasks, and stresses potential challenges and pitfalls during the lab. Students use the lab sessions to complete hands-on tasks. The lab tasks are scaffolded into several levels. Sometimes, the instructor supplements additional hints and examples in lab manuals to ease the learning curve. Finally, students are asked to answer post-lab questions and voluntarily complete a survey, which helps the instructors to evaluate the lab and further improve labs in the next iteration.

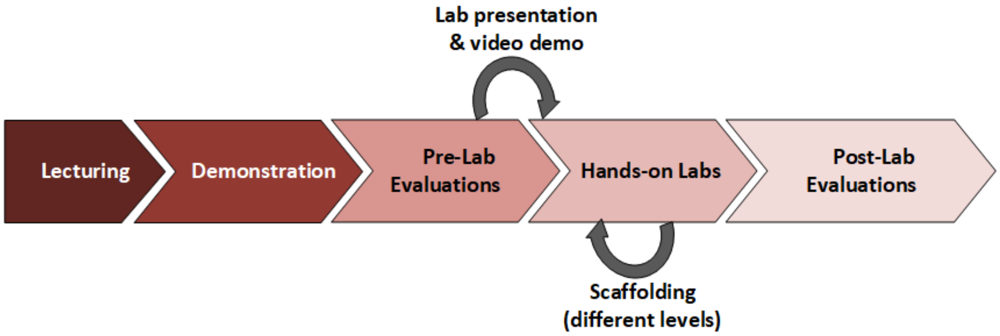


Figure 5: The process of conducting a lab.

Table 4: Questions used in post-lab surveys.

Questions	RQ mapping
1) The overall satisfaction with the lab.	1
2) The satisfaction in applying the technology and tools.	1
3) The understanding of learning objectives.	1
4) The familiarity in applying technology and tools *before* and *after* the lab.	2
5) The willingness to learn more about cybersecurity.	2
6) The overall interest in cybersecurity.	2
7) The background information is clear.	3
8) The instruction is clear.	3
9) The difficulty level is reasonable.	3
10) The lab is interesting.	3
11) The time spent on learning is worthwhile.	3
12) The approximate time spent (in hours).	3
13) What do you like most about this lab?	3
14) What do you like least about this lab?	3

5.2 Student Background

Between the Fall of 2018 and the Summer of 2022, we conducted assessments at two U.S. four-year institutions. The total number of voluntary participants is 287, of which 198 participants were from Institution 1 and 89 participants were from Institution 2. Figure 4 depicts some similar and distinct aspects of students' composition. First, most students who took hands-on labs and voluntary assessments are seniors (94% in Institution 1 and 98% in Institution 2) (Figure 4a) because most cybersecurity courses were arranged at the senior level. However, ethnic groups and academic backgrounds are different in the two institutions. For example, in Institution 1, 67% of the respondents are white, 18% are Asian, and 6% are African American. On the other hand, 49% of the respondents from Institution 2 are white, 24% are Hispanic, and 22% are Asian (Figure 4b). In addition, due to the different curricular requirements, 50% respondents from Institution 1 are IT major students, whereas 94% of respondents from Institution 2 are CS or CE major students (Figure 4c). Students' distinct ethnicity and academic backgrounds positively prepare us to answer pedagogic research questions in the next section.

5.3 Assessment and Surveys Questions

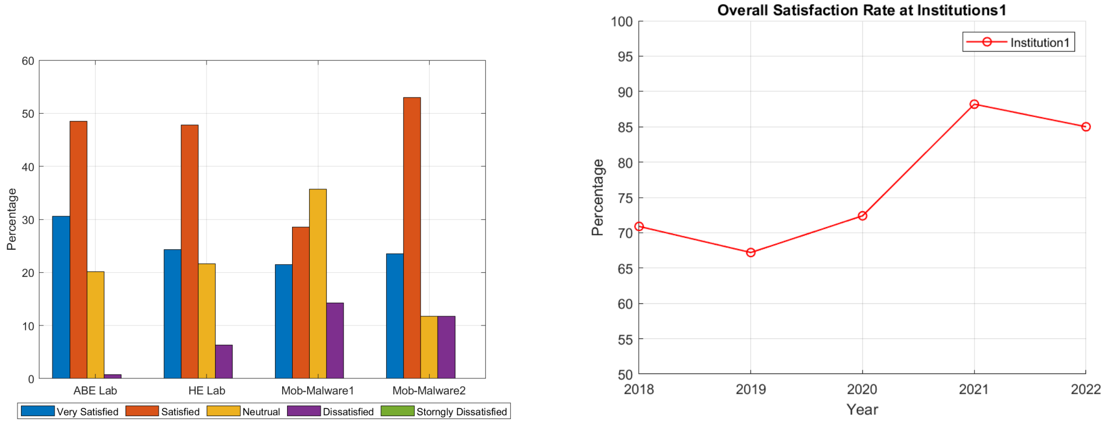
Our assessment contains *objective* and *subjective* questions. For objective questions, we adopt evaluation criteria as described in literature[35,24,5], which are tabulated in Table 4. In particular, we measure *effectiveness* criteria of students' learning outcomes (Questions 1 - 6) and *efficiency* criteria for the quality of lab materials (Questions 7 - 11). We employ a 5-point Likert scale, including options such as *Strongly agree*, *Agree*, *Neutral*, *Disagree*, and *Strongly disagree*. We interpret *Strongly agree* and *Agree* as positive feedback, while *Disagree* and *Strongly disagree* are considered negative feedback. In addition, we include open-ended *subjective* (SV) questions (Questions 12 - 14) to gather students' comments and suggestions, which will help us improve our materials in the future.

Prior research has demonstrated the following findings: 1) most students found the ReScuE environment easy to use; 2) students' knowledge of cybersecurity was significantly improved; and 3) students' interest in cybersecurity increased substantially after engaging in the labs[24]. To further the research, our assessment specifically attempts to answer three pedagogical research questions (RQs) as follows:

1. **RQ1**: What are the positive feedback rates (the percentage of students who are satisfied or strongly satisfied) for the ReScuE labs over five years at two institutions?
2. **RQ2**: How do the ReScuE and its labs effectively improve students' learning outcomes?
3. **RQ3**: Which factors are crucial and can significantly increase students' learning interests and improve their academic performance?

In particular, we first use answers to Questions 1 - 3 to address RQ1. Then, we use the results of Questions 4 - 6 and pre- and post-lab questionnaires to address RQ2. Finally, we use answers to Questions 7 - 15 to address RQ3 because we think they reflect students' needs, which will help us improve the quality of lectures and hands-on labs.

6 Results of Assessment



(a) Question 1

(b) Satisfaction Trend in Institution 1

Figure 6: Aggregated students' responses to Questions 1 and the satisfaction itrend in Institution 1

6.1 Research Findings

To demonstrate our findings and answer RQs without losing generality, we chose four labs we constantly offered students. To answer RQ1, we conducted the assessments to measure a) the students' overall satisfaction with the ReScuE labs and b) the clarity of the lab instructions. Figure 6a shows that most students provide positive feedback towards four ReScuE labs[2]. The satisfaction rates range between 79% and 57%. In addition, over five years, Institution 1 traces students' satisfaction rates, which are above 70% except for 2019 in Figure 6b. Due to the space constraint,

[2] We omitted *Mobile_SQLIA Lab* and *Cloud exploit & forensics lab* because they are not always be given over five years.

we do not include the results of other questions relevant to RQ1, because they demonstrate similar statistics.

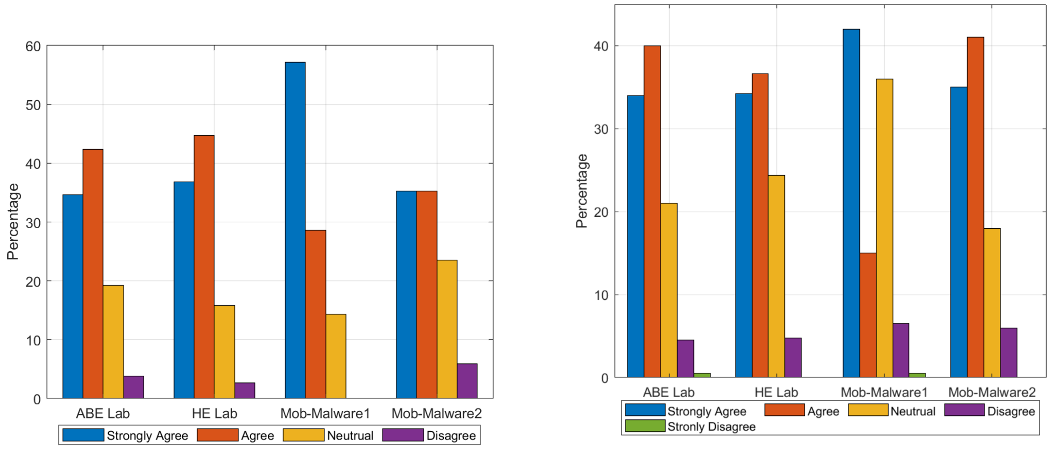
To answer RQ2, we use objective and subjective metrics to evaluate the effectiveness of labs: 1) whether students' proficiency in particular KUs significantly improves after taking labs and 2) whether students become more interested and confident in learning cybersecurity. Answering this question is crucial because it will give us insights on improving broader adoption and out-research efforts of disseminating the developed material. To provide a baseline of comparison, we asked several multiple-choice questions with similar challenge levels pre- and post-labs. The student's grades were averaged and categorized into four levels (Level 1 - 4), as denoted by "***Level 1**: No Proficiency (60 and below)*", "***Level 2**: Little Proficiency (61 - 70)*", "***Level 3**: Some Proficiency (71 - 85)*", and "***Level 4**: High Proficient (85 and above)*", respectively. Our analysis leads to at least two exciting findings. First, students' proficiency in KUs significantly improves after taking labs. Table 5 compares students' proficiency before and after taking hands-on labs at both institutions. Students' grades demonstrate a significant improvement after taking labs. For instance, after taking the "ABE Lab", the percentage of students changed from 0% to 48.2% (for Level 3) and from 0% to 25.9% (for Level 4). Similar improvements are apparent for all other labs in both institutions.

Table 5: The comparison of students' grades as the assessment metric of their technical proficiency (B)efore and (A)fter taking hands-on labs (in percentage) at Institution 1 and Institution 2.

Students' Proficiency	ABE Lab		HE Lab		Malware_Dev Lab		Malware_Ana Lab	
Level	B	A	B	A	B	A	B	A
Institution 1								
1	1.9	79.3	4.5	78.9	3.9	71.4	11.8	68.8
2	20.7	24.7	21.1	53.9	7.1	42.9	25	41.2
3	0	48.2	0	34.6	14.3	35.7	6.3	35.3
4	0	25.9	0	7.1	7.1	7.7	0	11.8
Institution 2								
1	6.3	81.3	4.5	86.4	7.1	71.4	11.8	68.8
2	18.8	56.3	13.6	40.9	7.1	35.7	25	35.3
3	0	31.3	0	40.9	14.3	42.9	6.3	41.2
4	0	6.3	0	13.6	7.1	14.3	0	11.8

Second, students become more interested and confident in learning cybersecurity. Figure 7a shows that between 70.6% and 85.7% of the students from Institution 1 agree that they became more interested in cybersecurity after taking labs. At Institution 2, the range is between 57% and 76%, as illustrated in Figure 7b. Both results demonstrate that students progressively build their professional expertise and self-confidence in cybersecurity through systematic training with hands-on labs.

While developing and refining lab manuals, we continuously improve many factors, including clear background information, illustrative examples, explicit instructions, and reasonable difficulty levels and durations. Thus, most students provide positive feedback on the clarity of lab manuals



(a) Institution 1

(b) Institution 2

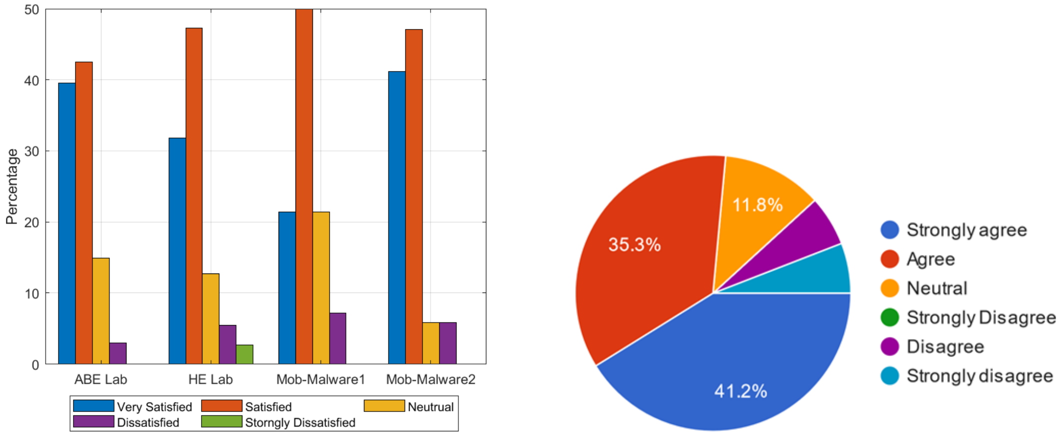
Figure 7: Students' responses to Question 6 at Institutions 1 and 2.

(Question 8), as illustrated in Figure 8a. However, we observe that some factors are more crucial than others. If improved, they can significantly improve students' interest and learning effect. In particular, two subjective questions (*SV1* and *SV2*) that collect students' feedback on the usability and challenges are especially helpful to answer RQ3. According to their feedback, the challenges included but were not limited to 1) lacking powerful computers for setting up the lab environment; 2) lacking human assistants; and 3) lacking timely feedback from the TAs and instructors. To tackle these challenges, we take three tactic solutions. First, we replace VMs with Docker containers and mobile emulators, which are computationally less expensive. The containers run YAML files to configure and compose a self-contained container that minimizes students' effort in setting up the lab environment. Second, to assist students, we recorded the pre-lab presentation and demonstration for each lab. The video clearly describes learning objectives, demonstrates technology and tools, identifies common pitfalls, and articulates deliverables. As illustrated in Figure 8b, 76.5% of the students from both institutions positively confirm the effectiveness of presentations and videos. Finally, to address students' concerns about timely feedback, we use the chat feature of Slack chatbot[36] and Zoom[37] to facilitate Q&A sessions. Because of these efforts, we kept students' satisfaction consistent during and after the Pandemic.

7 Reflections and Future work

After conducting a 5-year pedagogic project, we have gained valuable insights from both students and faculty in cybersecurity. In the following, we have compiled a list of lessons learned and recommendations for researchers and educators.

- *Does ethnicity, grades, or majors play an important role in practicing ReScuE labs* Despite diverse backgrounds among students from two institutions, we found no significant differences in learning outcomes. Our research suggests that prior knowledge of cybersecurity fundamentals, such as cryptography and access control, is more important than factors like ethnicity, grades, or



(a) Question 8

(b) Question 13

Figure 8: Aggregated students' responses to Questions 8 and 13.

major. It is worth noting that our study did not include first- and second-year college students.

- *Does the computer language help students complete hands-on practice more efficiently?* Although we do not require specific programming languages, some students have difficulty completing tasks due to limited knowledge of Python, Shell commands, and Java. This can impact the labs' adoption negatively. We suggest two solutions: providing pre-built software modules with functional code or intentionally leaving incomplete modules for students to complete using suggested APIs. Both options make labs more accessible for students who need help with programming.

- *Shall we set up everything for students?* Throughout the study, we always strive to let students focus on cybersecurity problem-solving and minimize the hassle of environment setup. For example, we prepare containers ready to go to each lab. Meanwhile, we try to balance between *what we have to do* and *what we can do*. Thus, we intentionally leave some environment setup tasks open for IT major students to enhance their problem-solving skills.

- *Is the cloud-based environment mandatory for all ReScuE labs?* Although the ReScuE framework is mainly based on CloudLab, the construction of a virtual environment in CloudLab is non-trivial. Students often encounter issues such as unavailable resources, an unexpectedly long time to deploy the environment, and network instabilities. Moreover, it could be challenging for instructors to run commands and programs in CloudLab without having solid experience in software-defined networking (SDN) and CloudLab. Thus, we redesigned some lab modules to allow educators to choose whether to use CloudLab based on their situations.

- *What else can we do to improve students' engagement and broader adoption of ReScuE?* Motivated by prior efforts that strive to increase students' awareness and interests in cybersecurity at the early stage[38], create interdisciplinary courses and modules for students at all levels[39], and broaden the diversity of participants[40], we can take the following measures to achieve this goal:. First, we will integrate ReScuE Labs modules into non-cybersecurity majors and general education courses like the best practices of security injections[38]. Second, we will make ReScuE labs more accessible to students in non-STEM majors, such as business and nursing, who need to know supply-chain security and privacy-preservation concepts. Third, we will customize ReScuE

Labs demonstrations, short video clips, and animations and make them approachable to K–12 students. Last but not least, we have made ReScuE, both instructor and user manuals, open-source and available to the public.

8 Conclusion

This paper presents ReScuE, a cloud-based framework, and a suite of hands-on labs designed to teach cybersecurity in pervasive computing. We continuously refined the software and instructions over multiple iterations and conducted formal evaluations at two institutions in five years. Our goal was to bridge the gap in cybersecurity education by conducting pedagogical research and gathering student feedback. The results showed that the ReScuE labs received positive feedback from students with diverse backgrounds and achieved high learning outcomes when used for online teaching and learning. To maximize the broader impacts, we have publicly made the ReScuE lab materials available.

References

[1] Dmitry Duplyakin, Robert Ricci, Aleksander Maricq, Gary Wong, Jonathon Duerig, Eric Eide, Leigh Stoller, Mike Hibler, David Johnson, Kirk Webb, Aditya Akella, Kuangching Wang, Glenn Ricart, Larry Landweber, Chip Elliott, Michael Zink, Emmanuel Cecchet, Snigdhaswin Kar, and Prabodh Mishra. The design and operation of CloudLab. In *2019 USENIX Annual Technical Conference (USENIX ATC 19)*, pages 1–14, Renton, WA, July 2019. USENIX Association. ISBN 978-1-939133-03-8.

[2] Bernard Ferguson, Anne Tall, and Denise Olsen. National cyber range overview. In *2014 IEEE Military Communications Conference*, pages 123–128. IEEE, 2014.

[3] John Wroclawski, Terry Benzel, Jim Blythe, Ted Faber, Alefiya Hussain, Jelena Mirkovic, and Stephen Schwab. *DETERLab and the DETER Project*. Springer International Publishing Switzerland, 2016.

[4] Mark Berman, Jeffrey S Chase, Lawrence Landweber, Akihiro Nakao, Max Ott, Dipankar Raychaudhuri, Robert Ricci, and Ivan Seskar. GENI: A federated testbed for innovative network experiments. *Computer Networks*, 61 (0):5–23, March 2014.

[5] Younghee Park, Hongxin Hu, Xiaohong Yuan, and Hongda Li. Enhancing security education through designing SDN security labs in CloudLab. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, SIGCSE '18, page 185–190, New York, NY, USA, 2018. Association for Computing Machinery.

[6] Richard S. Weiss, Stefan Boesen, James F. Sullivan, Michael E. Locasto, Jens Mache, and Erik Nilsen. Teaching cybersecurity analysis skills in the cloud. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education, SIGCSE 2015, Kansas City, MO, USA, March 4-7, 2015*, pages 332–337. ACM, 2015.

[7] Jean-François Lalande, Valérie Viet Triem Tong, Pierre Graux, Guillaume Hiet, Wojciech Mazurczyk, Habiba Chaoui, and Pascal Berthomé. Teaching Android mobile security. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, SIGCSE '19, page 232–238, New York, NY, USA, 2019. Association for Computing Machinery.

[8] Amazon LLC. Amazon web services. `https://aws.amazon.com/`, Accessed: February 8, 2023.

[9] Microsoft. Microsoft Azure services platform. `https://azure.microsoft.com/en-us/`, February 8, 2023.

[10] Xenia Mountrouidou and Vic Thomas. Cyberpaths: Cyber security labs for liberal arts institutions using the NSF global environment for network innovations (GENI). In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, pages 1241–1241, 2019.

[11] Mhd Wael Bazzaza and Khaled Salah. Using the cloud to teach computer networks. In *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, pages 310–314. IEEE, 2015.

[12] Khaled Salah. Harnessing the cloud for teaching cybersecurity. In *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, pages 529–534, 2014.

[13] Wenliang Du. SEED labs: Using hands-on lab exercises for computer security education (abstract only). In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, SIGCSE '15, page 704, New York, NY, USA, 2015. Association for Computing Machinery. ISBN 9781450329668.

[14] Kief Morris. *Infrastructure as code: Managing servers in the cloud.* O'Reilly Media, Inc., 1st edition, 2016. ISBN 1491924357.

[15] Cuong Pham, Dat Tang, Ken-ichi Chinen, and Razvan Beuran. CyRIS: A cyber range instantiation system for facilitating security training. In *Proceedings of the 7th Symposium on Information and Communication Technology*, pages 251–258, 2016.

[16] Jan Vykopal, Radek Ošlejšek, Pavel Čeleda, Martin Vizvary, and Daniel Tovarňák. Kypo cyber range: Design and use cases. In *Proceedings of the 12th International Conference on Software Technologies*, pages 310–321. SciTePress, 2017.

[17] Enrico Russo, Gabriele Costa, and Alessandro Armando. Building next generation cyber ranges with CRACK. *Computers & Security*, 95:101837, 2020.

[18] Maria Leitner, Maximilian Frank, Wolfgang Hotwagner, Gregor Langner, Oliver Maurhart, Timea Pahi, Lenhard Reuter, Florian Skopik, Paul Smith, and Manuel Warum. AIT cyber range: flexible cyber security environment for exercises, training and research. In *Proceedings of the European Interdisciplinary Cybersecurity Conference*, pages 1–6, 2020.

[19] Muhammad Mudassar Yamin and Basel Katt. Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security*, 116:102635, 2022.

[20] Philip Huff, Sandra Leiterman, and Jan P. Springer. Cyber arena: An open-source solution for scalable cybersecurity labs in the cloud. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, SIGCSE 2023, New York, NY, USA, 2023. Association for Computing Machinery.

[21] The OpenStack project. OpenStack Stein API Reference Documentation. `https://docs.openstack.org/stein/api/`, Accessed: February 8, 2023.

[22] Valdemar Švábenskỳ, Jan Vykopal, and Pavel Čeleda. What are cybersecurity education papers about? a systematic literature review of SIGCSE and ITiCSE conferences. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, pages 2–8, 2020.

[23] Joint Task Force on Cybersecurity Education. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Association for Computing Machinery, New York, NY, USA, 2018. ISBN 9781450389198.

[24] Anyi Liu, Dong Han, and Huirong Fu. ReScuE: A cloud-based system for cybersecurity education and training. In *The 22nd Colloquium on Information Systems Security Education (CISSE'18)*, 2018.

[25] David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. *Metasploit: The Penetration Tester's Guide*. No Starch Press, San Francisco, CA, USA, 1st edition, 2011. ISBN 159327288X, 9781593272883.

[26] Greenbone Networks. OpenVAS - open vulnerability assessment scanner. http://www.openvas.org/, Accessed: February 8, 2023.

[27] Rapid7. Metasploit: A penetration testing software. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1240, Accessed: February 8, 2023.

[28] Volatility. Volatility Foundation. https://www.volatilityfoundation.org/, Accessed: February 8, 2023.

[29] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 321–334, 2007.

[30] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, page 89–98, New York, NY, USA, 2006. Association for Computing Machinery.

[31] Steven Arzt, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves Le Traon, Damien Octeau, and Patrick McDaniel. FlowDroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. In *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI '14, page 259–269, New York, NY, USA, 2014. Association for Computing Machinery.

[32] Ajin Abraham and Magaofei and Matan Dobrushin and Vincent Nadal . Mobile Security Framework (MobSF). https://github.com/MobSF/Mobile-Security-Framework-MobSF, Accessed: February 8, 2023.

[33] Google LLC. VirusTotal. https://www.virustotal.com/gui/home/upload, Accessed: February 8, 2023.

[34] Wikipedia. Wikipedia, the free encyclopedia, Accessed: February 8, 2023. URL http://en.wikipedia.org.

[35] Wenliang Du and Ronghua Wang. SEED: A suite of instructional laboratories for computer security education. *J. Educ. Resour. Comput.*, 8(1), 2008. ISSN 1531-4278.

[36] Slack. https://slack.com/, Accessed: February 8, 2023.

[37] Zoom Video Communications, Inc. https://zoom.us/, Accessed: February 8, 2023.

[38] Blair Taylor and Sidd Kaza. Security injections@Towson: Integrating secure coding into introductory computer science courses. *ACM Transactions on Computing Education*, 16:1–20, 06 2016.

[39] Richard Weiss, Xenia Mountrouidou, Stacey Watson, Jens Mache, Elizabeth Hawthorne, and Ankur Chattopadhyay. Cybersecurity across all disciplines in 2020. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, pages 1404–1404, 2020.

[40] Xenia Mountrouidou, David Vosen, Chadi Kari, Mohammad Q. Azhar, Sajal Bhatia, Greg Gagne, Joseph Maguire, Liviana Tudor, and Timothy T. Yuen. Securing the human: A review of literature on broadening diversity in cybersecurity education. In *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, ITiCSE-WGR '19, page 157–176, New York, NY, USA, 2019. Association for Computing Machinery. ISBN 9781450375672.