UCLP: A Novel UAV Cybersecurity Laboratory Platform

Ashok Raja
University of Massachusetts Dartmouth
North Dartmouth, USA
araja1@umassd.edu

Julio Galvan
California State University San Marcos
San Marcos, USA
galva057@cougars.csusm.edu

Yanyan Li
California State University San Marcos
San Marcos, USA
yali@csusm.edu

Jiawei Yuan
University of Massachusetts Dartmouth
North Dartmouth, USA
jyuan@umassd.edu

ABSTRACT

Recent years have witnessed a rapid development of unmanned aerial vehicles (UAVs) and their applications in various fields. At the same time, the utilization of UAVs also raises serious security and safety concerns. Given a large number of UAV-related jobs to be created in the near future, it is pressing to educate and train current and next-generation cybersecurity professionals towards UAVs and their applications. However, there is a lack of education and training materials on UAV cybersecurity, especially for hands-on practice. In this paper, we propose a novel UAV cybersecurity laboratory platform (UCLP), which provides efficient and effective hands-on practice. UCLP offers not only a cost-effective UAV cybersecurity practice environment, but also a series of designed and pre-configured lab modules. UCLP adopts a plug-in based design and hence supporting flexible customization of existing and new lab modules. UCLP uses technical solutions to overcome non-technical limitations in UAV cybersecurity practice (e.g., regulations of UAV operations). Our evaluation results demonstrated the efficiency, flexibility, and effectiveness of UCLP and indicated UCLP is promising to be integrated into the education and training of UAV, cybersecurity, and related fields.

CCS CONCEPTS

• **Applied computing** → **Interactive learning environments**; • **Security and privacy**; • **Computer systems organization** → **Robotics**;

KEYWORDS

UAV, Security, Laboratory, Instructional Operating System

ACM Reference Format:
Ashok Raja, Julio Galvan, Yanyan Li, and Jiawei Yuan. 2021. UCLP: A Novel UAV Cybersecurity Laboratory Platform. In *Proceedings of the 22nd Annual Conference on Information Technology Education USB Stick (SIGITE '21), October 6–9, 2021, Snowbird, UT, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3450329.3476852

SIGITE '21, October 6–9, 2021, Snowbird, UT, USA.

ACM ISBN 978-1-4503-8355-4/21/10…$15.00
https://doi.org/10.1145/3450329.3476852

1 INTRODUCTION

Alongside the rapid development in aviation, sensing, artificial intelligence, and software and hardware technologies, a revolution has been powered for UAVs and unmanned aerial system (UAS). In recent years, UAVs have demonstrated their promising capabilities to facilitate applications in a spectrum of military and civilian applications, including remote sensing, search-and-rescue, infrastructure inspection, shipping and delivery, and precise agriculture. According to the report from the Association for Unmanned Vehicle Systems International (AUVSI) [1], 100,000 UAV-related jobs are estimated to be created by 2025, which will contribute $82 billion to the U.S. economy. However, the pervasive utilization of UAVs also has raised serious cybersecurity concerns about their threats. UAVs are now being looked upon as an emerging cybersecurity issue in both as targets for cyber-attack and as potential attack vectors for malicious actors. Therefore, educating, training, and enhancing current and next-generation cybersecurity professionals towards UAVs and their applications via effective, affordable, and scalable mechanisms is highly demanded.

Currently, there is a lack of education and training materials on UAV cybersecurity. While several attempts have been made towards designing courses for UAVs [2–5], they are designed from the perspectives of control, design, and applications. Inadequate integration of UAVs with cybersecurity as well as the lack of hands-on practice all make the learning insufficient and ineffective. Hands-on cybersecurity practices are indispensable to the education and training of cybersecurity. However, the design and development of hands-on practices for UAV cybersecurity face unique challenges that come from not only how to integrate cybersecurity techniques but also the regulations of UAV operations. To be specific, the Federal Aviation Administration (FAA) requires Remote Pilot Certificate to fly drones under the FAA's Small UAS Rule (Part 107) [6]. The FAA's Rules of the Sky also defines that flying UAVs in certain areas is prohibited [7]. Currently, most students do not have the required Pilot Certificate during the study and not all institutions have nearby authorized UAV flying zones. Such a fact significantly restricts the environment for the education and training of UAV cybersecurity.

In this paper, we propose to use technical solutions to overcome these non-technical limitations in UAV cybersecurity education,

and then enable hands-on exercises to be carried out at locations with limited UAV cybersecurity resources and conditions. To the best of our knowledge, UCLP is the first hands-on laboratory platform designed for UAV cybersecurity education and training. In particular, we developed a novel *UAV Cybersecurity Laboratory Platform* named UCLP, which simulates different UAV flying scenarios with the integration of cybersecurity components. UCLP provides a series of carefully designed hands-on UAV cybersecurity lab modules. With UCLP, students are not only able to perform different cybersecurity attack/defense tasks towards UAV, but also visualize these attacks and defenses to understand their impact on UAV operations to obtain a deep understanding. UCLP offers a standard mode and an advanced mode. In the standard mode, users can practice our pre-configured lab modules and tasks. The advanced mode offers APIs for expert users and instructors to customize existing lab modules and even add their own modules. UCLP integrates and pre-configures all necessary components into a virtual machine instance, and hence supporting easy and fast deployment on a stand-alone computer. To evaluate the efficiency and effectiveness of UCLP, we conduct a survey with the participation of 30 users, which include instructors, professionals, and students from different majors. Our evaluation results are very positive in general and indicate that UCLP can be leveraged to promote the education and training of UAV, cybersecurity, and other related fields.

The rest of this paper is organized as follows: We briefly describe the related work in Section 2. We then present the design of UCLP in Section 3 and its implementation in Section 4. We detail the evaluation of UCLP in Section 5 and conclude this paper in Section 6.

2 RELATED WORK

During the past decade, there is a growing development of cybersecurity programs and courses in many universities. Although existing cybersecurity curriculum materials have covered a wide range of topics, materials to support the education and training of UAV security are largely missing, especially considering the increasing attention raised to the security issues of UAV and UAS [8]. There are also several curriculum materials that have been developed for UAV and UAS [2–5]. Nevertheless, these existing materials focus on the operation, control, design, deployment, or applications of UAV and UAS, in which security issues are not taken into consideration or are only treated as special topics with very limited coverage. In recent years, an increasing amount of research attempts have been to address security issues of UAVs [9–11], however, the corresponding effort spent on developing educational materials and tools are limited.

To enable effective and convenient hands-on security practices, many tools have been proposed and used in security education and training by applying virtualization technologies. These tools can be roughly classified into three categories according to their architectural models, i.e., hosted hypervisor-based [12, 13], bare metal hypervisor-based [14, 15], and cloud-based [16, 17]. Considering the support of UAV security practice, these existing tools become inappropriate, since none of them involves the necessary UAV software and hardware components. Another line of related technologies is the UAV simulation tool [18–20]. These simulators are mainly designed to support the evaluation of UAV flying test, and do not include security modules.

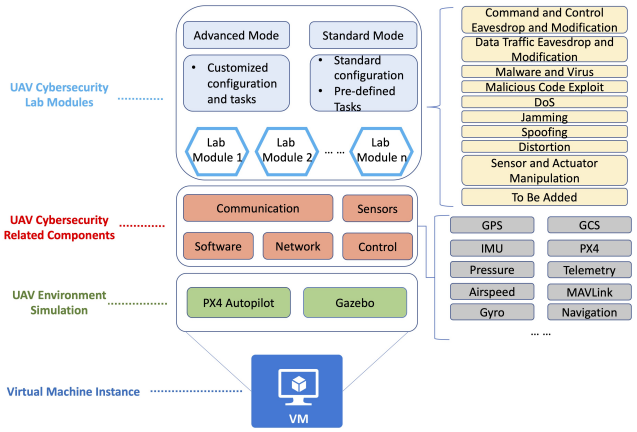

Figure 1: Design Overview of UCLP

3 SYSTEM DESIGN

The design overview of UCLP is presented in Fig.1. UCLP is developed mainly using software simulation, which provides low-cost but effective UAV simulation environment with the support of different UAV models, UAV communication and network models, satellite models, and sensors. In addition, UCLP also supports hardware-in-the-loop (HIL) simulation, which is the closest to the actual flight without actually flying. On top of the UAV software/hardware simulation environment, a series of hands-on cybersecurity exercise modules are developed to cover UAV cybersecurity issues from different angles.

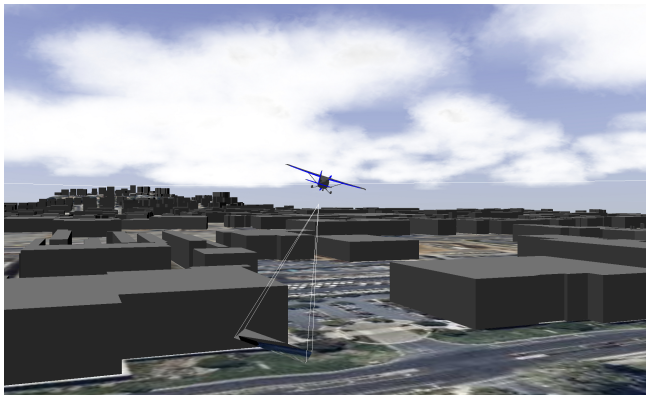

Figure 2: An Example of Simulated UAV Flying Environment in UCLP

The design of UCLP utilizes PX4 Autopilot [21] and Gazebo simulator [22] as the basic UAV simulation framework, in which various flying environments and UAV models (e.g., quadcopter, multicopter, and fixed-wing) are provided as an example shown in Fig.2. Additional customized UAV models and flying environment can also be

added when necessary. On top of the basic framework, UCLP investigates major areas of UAVs that can be vulnerable to cybersecurity attacks, including communication, sensors, network, control, and software. In each area, different components are further explored to integrate cybersecurity attack and defense modules. For example, the communication area includes telemetry, MAVlink, GPS, and UAV to UAV communication in the current design of UCLP. For each type of cybersecurity attack, UCLP designs a corresponding hands-on lab module with instructions and lab tasks. To enable easy and fast deployment, UCLP integrated all necessary components and configurations into a virtual machine instance, which is ready-to-use on most stand-alone computers without additional hardware and cost.

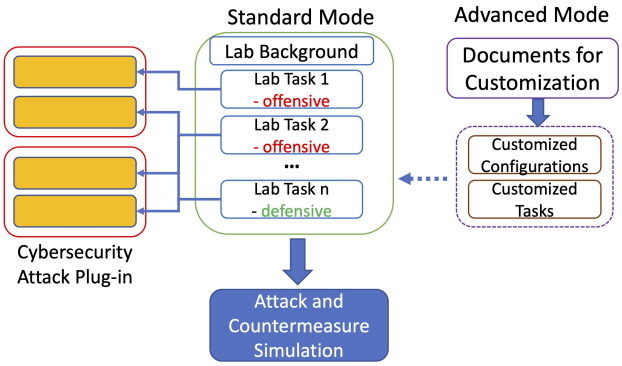

Figure 3: Design of Lab Module

In UCLP, we adopt a plug-in based design for cybersecurity lab modules as shown in Fig.3. Specifically, the codes and configurations needed for the simulation of a cybersecurity attack/defense will be embedded into the plug-ins of the corresponding UAV components, which are loaded and added into the base UAV simulate framework when the lab module is launched. With such a design, the execution of each lab module only needs to load related plug-ins without affecting others, and hence making UCLP support quick restore after the completion of each lab module. During the design of each lab, we first provide an overall background introduction and necessary materials. Then, lab tasks are designed with a balanced coverage of both offensive and defensive skills. Such a design will help students build a security mind using the threat-driven approach, i.e., students will learn the adversary's view and perspective of security, which are essential to understand security problems and then build countermeasures more effectively. The threat-driven approach implies the destructive thinking as a comparison to the traditional constructive thinking, i.e., how to break a system v.s. how to secure a system. The destructive thinking also matches the concept of inquiry-based learning - an effective form of active learning, as it motivates and facilitates students and instructors posing questions and scenarios to identify potential threats to UAVs.

Besides the pre-configured and designed lab tasks offered by our standard mode, UCLP also provides documentation for the customization of lab modules and tasks. Therefore, users with sufficient background knowledge (e.g., instructors and experienced professionals) are able to adjust the lab modules according to their needs and even create new lab modules. Thanks to our plug-in based design that separates the dependent plug-ins of each lab module, customized modules will not affect the execution of other existing lab modules. Therefore, the advanced mode in UCLP not only provides the flexibility of customization to users, but also benefits the long-term development of UCLP through collaborative development.

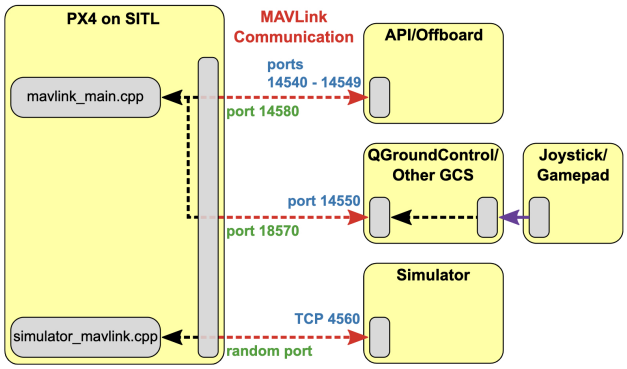

Figure 4: Overview of Simulation Environment [23]

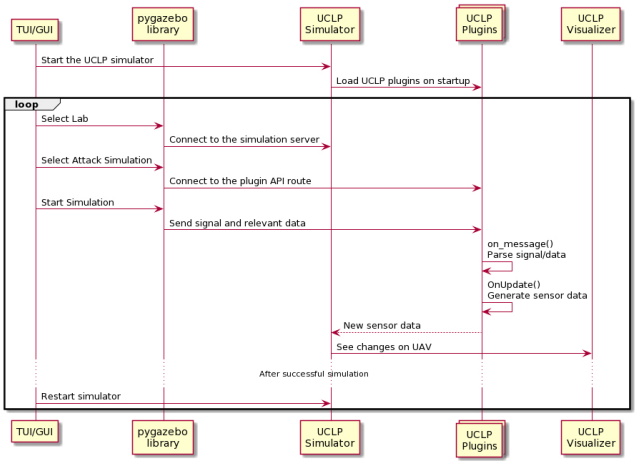

Figure 5: Plug-in based Implementation

4 IMPLEMENTATION

The base UAV simulation environment is developed using PX4 Autopilot [21] and Gazebo simulator [22] as shown in Fig.4. In addition, QGroundControl is adopted as the ground control station for UAVs [24]. The current version of UCLP provides a command-line-based user interface, developed using Python. The core cybersecurity modules are implemented using C++ with our plug-in based design shown in Fig.5. In a regular simulation (i.e., no attack situation), plug-ins in UCLP collect, generate, and update data for different components of UAVs and hence enabling the operations of UAVs in the simulated environment. For the implementation of a lab module,

a set of related Gazebo plug-ins are modified and implemented to enable the corresponding cybersecurity components required by the lab module. When a lab module in UCLP is launched, the corresponding plug-ins will be loaded to simulate attacking patterns based on the user's selections and inputs.

For example, by providing a customized GPS plug-in, UCLP is able to simulate GPS jamming attacks to the UAV, which stops updating the GPS sensor with new data when the attack is triggered as shown in Fig.6. As a result, the "no global position" warning is raised for the UAV as shown in the red box, and the failsafe mode is triggered as the countermeasure to land the UAV at the current location. Similarly, spoofing GPS attack can be simulated by providing modified GPS data to the UAV using the GPS plug-in as an example shown in Fig.7

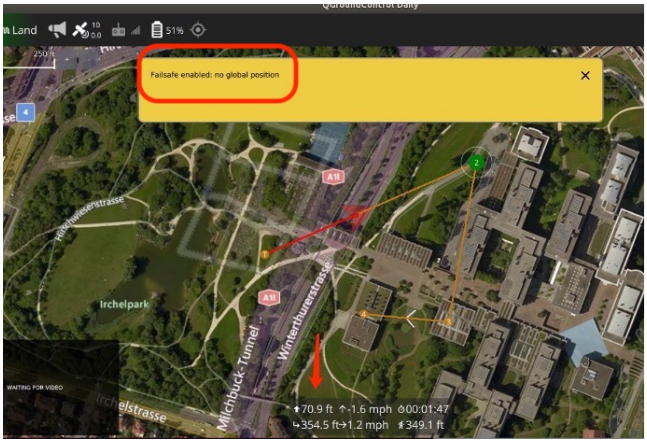

Figure 6: Example of GPS Jamming

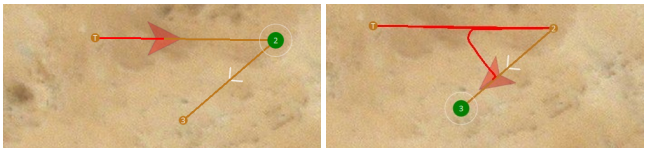

Figure 7: Example of GPS Spoofing (left: planned flying pattern without attack; right: spoofed flying pattern under attack)

Figure 8 is the code segment of our simulated attacks to the accelerometer and gyroscope of the UAV in the inertial measurement unit (IMU) plug-in. In this attack, our developed plug-in increases the accelerometer and gyroscope bias by different amounts of extra bias to simulate compromised sensors or sensors with error readings.

To avoid plug-ins in different modules affected with each other after each practice, our implementation includes a script to automatically restore all modified plug-ins in the current lab when a new lab-module is launched. Therefore, only the necessary plug-ins will be loaded to assure the correctness of each lab's execution. This implementation method also supports flexible customization to extend UCLP for additional lab modules, since plug-ins designed

```
if(accelerometer || gyroscope) {
    // TODO: Accept user input for the extra value
    for (int i = 0; i < 3; ++i) {
        if(accelerometer) {
            auto extra = standard_normal_distribution_(random_generator_);
            std::cout << "accel-bias=" << accelerometer_bias_[i] << " + extra-bias=" << extra << std::endl;
            accelerometer_bias_[i] = accelerometer_bias_[i] + extra;
        } else if(gyroscope) {
            auto extra = (standard_normal_distribution_(random_generator_) / 100) * 3;
            std::cout << "gyro-bias=" << gyroscope_bias_[i] << " + extra-bias=" << extra << std::endl;
            gyroscope_bias_[i] = gyroscope_bias_[i] + extra;
        }
    }
    if(accelerometer) accelerometer = !accelerometer;
    if(gyroscope) gyroscope = !gyroscope;
}
```

Figure 8: Code Segment of Sensors Attacks in the IMU Plug-in

and developed in these newly added lab modules will not mess up existing lab modules in UCLP.

5 EVALUATION

To evaluate the efficiency, effectiveness, and flexibility of UCLP, we collected feedback from 30 voluntary participants in April/May 2021. 6 of these volunteers are instructors and industry professionals, and the rest 24 are students from different majors, including computer science, computer engineering, software engineering, and aerospace engineering. Participants are provided with a link to download the virtual machine image of UCLP, an introduction video of UCLP, and a lab manual. For instructors and professionals, we also provide a manual for the customization of lab modules and tasks. We collect feedback from participants using a survey after they completed the following tasks: 1) watch an introduction video of UCLP, 2) setup UCLP using VMWare, 3) select one lab module and complete the lab tasks in it), and 4) customize a lab task or add a new lab module (optional). The survey used in our evaluation has 16 questions in total, of which 7 questions for all participants, 4 questions are for instructors and professionals only, and 5 questions are for student participants only. Likert scale is adopted for survey questions, i.e., strongly disagree, disagree, neutral, agree, and strongly agree. The survey questions are summarized in Table 1.

5.1 Evaluation Metrics

Our evaluation of UCLP focuses on two major factors: efficiency and effectiveness. The evaluation of efficiency mainly focuses on assessing the appropriateness and design of UCLP. This evaluation will help us identify the problems in our supporting manual, lab description, designs of lab tasks, and the design concepts of UCLP. With regards to the evaluation of effectiveness, we focus on the outcomes of students after they complete the lab tasks in UCLP. This evaluation will help us understand how effective UCLP is able to attract students to the learning in UAV and cybersecurity related fields and enhance their learning of these fields. The detailed metrics of each evaluation factor are summarized in Table 2.

5.2 Evaluation Results

The results of our survey are presented in Fig.9 to Fig.12. Overall, we can see that participants have very positive feedback about the efficiency and effectiveness of UCLP. As shown in Fig.9, the results of survey questions 1-5 indicate all participants are able to quickly set up and start UCLP for hands-on practice. Comparing

Table 1: Summary of Suvery Questions

Questions - All Participants
1. UCLP can be easily set up on your computer.
2. The process of accessing different modules in UCLP is straightforward and smooth.
3. It is easier and more cost-effective to use UCLP than building hardware-based experiment environment.
4. UCLP provides a convenient environment for UAV cybersecurity practice.
5. Using UCLP helps me save time on hardware and software configuration for lab exercises.
6. I have completed this lab exercise in less than 50 minutes
7. The difficultly of lab tasks are well balanced.
Questions - Students Only
8. I am interested in conducting more lab modules using UCLP.
9. I would like to use UCLP for the study of UAV, cybersecurity, or other related fields in the future.
10. I have a better understanding of the topics covered after completing the lab.
11. I am satisfied with the UAV and cybersecurity knowledge gained in this lab exercise.
12. I learned new skills for UAV cybersecurity by conducting the lab tasks.
Questions - Instructors and Professionals Only
13. The plug-in based design makes UCLP easy to customize labs.
14. I am able to create my own lab modules and tasks in UCLP.
15. I would like to contribute customized lab tasks or lab modules for more diverse UAV security labs for UCLP when possible.
16. I would like to use UCLP for teaching or training the workforce for UAV, cybersecurity, or other related fields.

Table 2: Summary of Evaluation Metrics

Efficiency
The time spent on setting up and using UCLP (Q1,Q2,Q4)
The effort compared with hardware-based practice (Q3,Q5)
The level of difficulty of lab tasks (Q6,Q7)
The usefulness of the supporting documents (Q2,Q13,Q14)
The difficulty of customizing lab modules and tasks (Q13,Q14)
Effectiveness
The level of interest in the lab modules and tasks (Q8,Q9)
The level of understanding of targeted learning topics (Q10)
The participants' perceptions of their learning (Q11)
The development of related skills (Q12)
The interest of contributing to UCLP (Q15)
The interest of using UCLP in related courses (Q16)

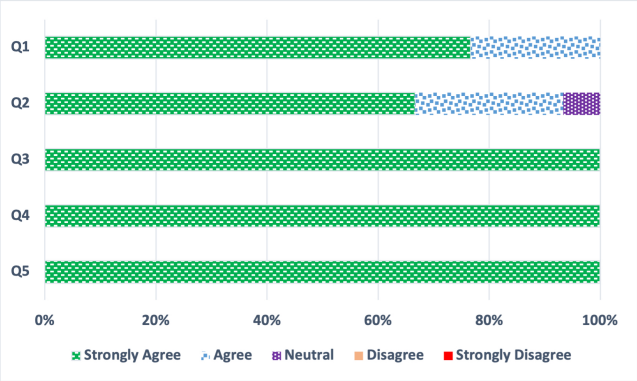

Figure 9: Survey Results of Q1-Q5

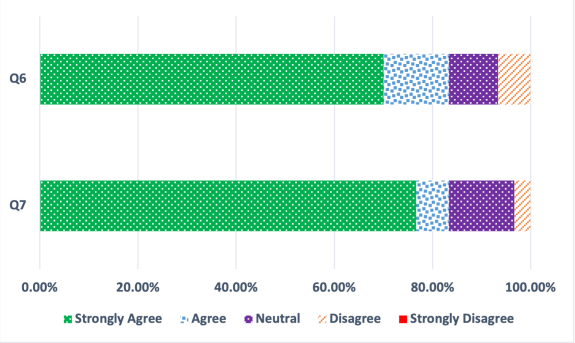

Figure 10: Survey Results of Q6-Q7

with hardware-based UAV experiment environment, UCLP is more cost-effective and can significantly save the time of configuration for users. Fig.10 presents the results of our questions about the difficulty of lab tasks in UCLP. Over 80% of participants satisfy the difficulty of lab tasks they completed using UCLP. There is also a small portion of participants consider the lab tasks are too difficult. According to our observation, our lab tasks become challenging for participants with no (or very limited) background knowledge. Therefore, we plan to use two strategies for the future design and development of UCLP lab tasks, i.e., 1) provide additional supporting materials to cover background knowledge; 2) add optional starting tasks in each lab module to help prepare users with limited background for the follow-up standard tasks.

Fig.11 summarizes the results of survey questions 8-12, which are for student participants only. The results of questions 8 and 9 indicate students have a strong interest in using UCLP for the learning of UAV, cybersecurity, and other related fields. For the learning effectiveness, about 90% of students satisfy the knowledge

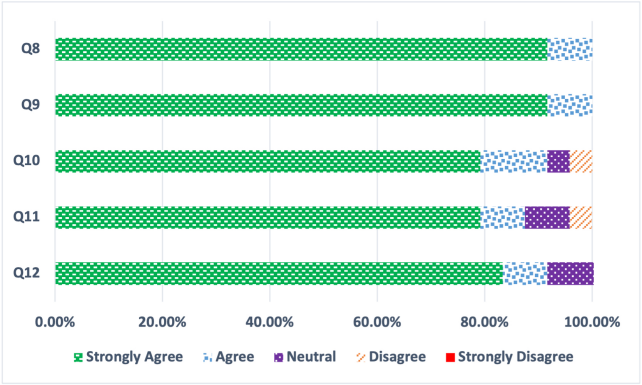

Figure 11: Survey Results of Q8-Q12

gained by conducting our lab tasks, which are reflected by a better understanding of related topics covered in the lab, and the new skills learned and practiced from the lab according to the results from Q10 to Q12. Therefore, it is promising to use UCLP for the education and training of UAV cybersecurity and related fields.

The results of Q13 and Q14 shown in Fig.12 demonstrate that instructors and professionals satisfy the plug-in based design in UCLP to customize lab modules and are able to create their own lab modules according to the supporting materials. In Q15 and Q16, instructors and professionals also show strong interest to contribute their customized lab modules to UCLP and adopt UCLP for their teaching and training. Therefore, it is promising to make UCLP an open-source platform and integrate the contribution from the community of UAV, cybersecurity, and other related fields.

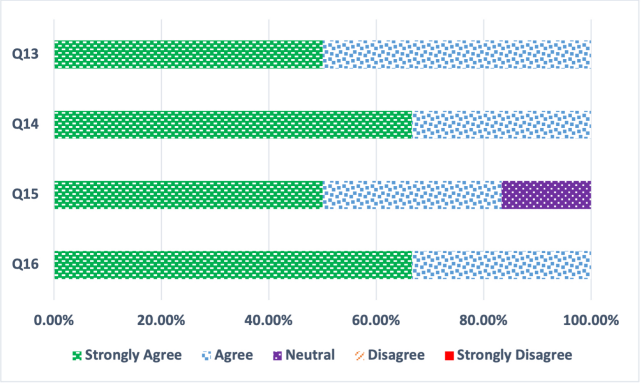

Figure 12: Survey Results of Q13-Q16

6 CONCLUSION

In this paper, a novel UAV cybersecurity laboratory platform named UCLP is proposed, which provides an efficient and effective hands-on environment to support the education and training of UAV, cybersecurity, and other related fields. UCLP can help institutions, instructors, professionals, students, and other users that are restricted by hardware, space, and regulations to conduct UAV cybersecurity education and experiments. UCLP integrates and pre-configures all necessary components into a virtual machine instance, and hence can be easily deployed on stand-alone computers. By adopting a plug-in based design, UCLP supports flexible customization for additional lab modules and tasks, which make it can be integrated into existing courses. Our evaluation results not only demonstrate the efficiency and effectiveness of UCLP, but also show strong interests from students, instructors, and professionals in using and contributing to UCLP. UCLP is expected to lower the barriers in UAV cybersecurity hands-on practices and promoting workforce development in the fields to help address the shortage of professionals.

ACKNOWLEDGMENTS

This work is supported by the US National Science Foundation awards (DGE-1956193 and CNS-2050972).

REFERENCES

[1] Association for Unmanned Vehicle Systems International. The Economic Impact of Unmanned Aircraft Systems Integration in the United States. http://www.auvsi.org/auvsiresources/economicreport.
[2] Qassim A. Abdullah. GEOG 892 Geospatial Applications for Unmanned Aerial Systems (UAS). https://www.e-education.psu.edu/geog892/syllabus.
[3] University of Maine at Augusta. UAS Courses. https://www.uma.edu/academics/programs/aviation/uas/.
[4] Embry-Riddle Aeronautical University. Bachelor of Science in Unmanned Aircraft Systems . https://erau.edu/degrees/bachelor/unmanned-aircraft-systems-science.
[5] Everglades University. Bachelor of Science Degree in Aviation/Aerospace | Concentration in Unmanned Aerial Systems (UAS). https://www.evergladesuniversity.edu/courses/unmanned-aerial-systems-degree/.
[6] Fact Sheet – Small Unmanned Aircraft Regulations (Part 107). https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615, 2018.
[7] FAA - Rules of the Sky. https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_101/, 2018.
[8] The White House. National Strategy for Aviation Security. https://www.whitehouse.gov/wp-content/uploads/2019/02/NSAS-Signed.pdf.
[9] Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang, and Hal Aldridge. *Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles.*
[10] Yueyan Zhi, Zhangjie Fu, Xingming Sun, and Jingnan Yu. Security and privacy issues of uav: A survey. *Mobile Networks and Applications*, Jan 2019.
[11] C. G. L. Krishna and R. R. Murphy. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pages 194–199, Oct 2017.
[12] Wenliang Du and Ronghua Wang. Seed: A suite of instructional laboratories for computer security education. *J. Educ. Resour. Comput.*, 8(1):3:1–3:24, March 2008.
[13] R. Harrison Wagner. Designing a network defense scenario using the open cyber challenge platform. 2013.
[14] Weiqing Sun, Varun Katta, Kumar Krishna, and R. Sekar. V-netlab: An approach for realizing logically isolated networks for security experiments. In *Proceedings of the Conference on Cyber Security Experimentation and Test*, CSET'08, pages 5:1–5:6, Berkeley, CA, USA, 2008. USENIX Association.
[15] Yanyan Li and Mengjun Xie. Platoon: A virtual platform for team-oriented cybersecurity training and exercises. In *Proceedings of the 17th Annual Conference on Information Technology Education*, SIGITE '16, pages 20–25, New York, NY, USA, 2016. ACM.
[16] Yanyan Li, Dung Nguyen, and Mengjun Xie. Ezsetup: A novel tool for cybersecurity practices utilizing cloud resources. In *Proceedings of the 18th Annual Conference on Information Technology Education*, SIGITE '17, pages 53–58, New York, NY, USA, 2017. ACM.
[17] L. Xu, D. Huang, and W. Tsai. Cloud-based virtual laboratory for network security education. *IEEE Transactions on Education*, 57(3):145–150, Aug 2014.
[18] Paparazzi UAS. https://github.com/paparazzi/paparazzi.
[19] FlightGear. https://www.flightgear.org/.
[20] A survey of open-source uav flight controllers and flight simulators. *Microprocessors and Microsystems*, 61:11 – 20, 2018.
[21] PX4 Autopilot. https://px4.io/.
[22] Gazebo Simulator. http://gazebosim.org/.
[23] PX4 User Guide - Simulation. https://docs.px4.io/master/en/simulation.
[24] QGroundControl. http://qgroundcontrol.com/.