University of Florida GenCyber Summer Camp: Hardware Security for High School Students

University of Florida proposes a Hybrid GenCyber Summer Camp: Hardware Security for High School Students. By leveraging the rich teaching and learning resources in Florida Institute for Cybersecurity Research (FICS Research), faculty members from College of Engineering, College of Education, and Center for Precollegiate Education and Training (CPET) will join forces to design an engaging summer camp focusing on hardware security for diverse high school students. The highlights of the camp are: (1) extending the cybersecurity education to hardware security for K-12 students; (2) leveraging existing educational toolkits developed by us to provide robust learning experience for students; (3) providing a versatile of pre/post camp activities to promote learning, interest development, and career awareness in cybersecurity; (4) utilizing a variety of evidence-based strategies to foster students' learning of cybersecurity.

The six principles of the GenCyber Cybersecurity Concepts were reinforced in the activities throughout the curriculum as shown in Table 3. These topics will be adapted from Ha-Ha board cybersecurity education platform to make it age-appropriate for high school students. Beyond this direction instruction hours, we will have two Friday afternoons (6 hours in total) to engage in post-secondary and career awareness activities, which students can visit FICS Research state of art facilities, interact with near peer undergraduate students, graduate students, and faculty members. Through the combination of direct instruction and extracurricular activities, this summer camp can meet the GenCyber program goals to not only increase students' knowledge and interest in cybersecurity but also promote diverse students' awareness of postsecondary and career opportunities.

To facilitate a learner-centered learning environment, we have a set of strategies: 1) Besides presentations, demos, and video tutorials, this camp is heavily using learning by doing for students to engage in hands-on activities. 2) Students will be put into groups for collaborative learning and each group will be assigned an undergraduate mentor. There is rich research evidence to show the learning effectiveness of collaborative learning and near-peer mentoring in K-12 education. 3) This camp will also employ contextualized learning strategies to improve students' engagement and interest in the curricula activities. For example, we will use a smartphone to demonstrate the hardware system for students to relate the curriculum content to their daily lives.

We will conduct two types of evaluation for the program. First, we will design formative assessments to monitor student learning and provide ongoing feedback to staff and students. Specifically, we will collect students' feedbacks on their learning experience and address their concerns promptly by assessing students' opinions (e.g., potential improvements for the course design, level of enjoyment, and satisfaction) with each learning activity. Meanwhile, short assessments for each learning activity will be designed with differentiated measures depending on students' feedbacks and content difficulty. Second, we will conduct summative assessments to evaluate students' learning outcomes at the end of the program. Specifically, we will assess the expected end outcomes of our proposed program, which are that participating students will become more interested in cybersecurity as a field of study, increase their understanding of cybersecurity, and reinforce their sense of self-efficacy and identity as a STEM individual.

This summer camp will leave a rich legacy. First, it will generate (to our knowledge) the first hardware security curriculum materials and tool kit for K-12 students with comprehensive support. We will open-source this curriculum resources for national use. Second, to foster continued cybersecurity awareness in the community, we will create social network service (SNS) groups (e.g., Facebook, Slack, etc.) to connect students, teachers, and parents interested in cybersecurity. Students who participate in our program and agree to connect will become the seed users in these interest groups. Third, this summer camp will help FICS Research at UF make a significant step towards building the *K-12 Cybersecurity Academy* which aims to continue to design and develop open-accessed project-based curriculum for K-12 students and provides free consultation to local K-12 stakeholders on opening courses or creating programs on cybersecurity. The proposed GenCyber hardware security program can potentially have a significant impact on the local community given there are limited learning resources in nearby schools.