Four Week Summer Program in Cyber Security for High School Students: Practice and Experience Report

Melissa Danforth (melissa@cs.csub.edu) and Charles Lam (clam@csub.edu)
California State University, Bakersfield

1 Introduction

Cyber security education and outreach is a national priority. It is critical to encourage high school students to pursue studies in cyber security and related fields. High school outreach is a fundamental component of a cohesive cyber security education program. Most high school outreach programs in cyber security focus on short-term events such as a capture the flag contest or the CyberPatriot competition. While a competitive event is engaging for high school students, it does not give a comprehensive overview of cyber security education and careers.

We explored the use of a four-week, hands-on, intensive summer program for engaging and encouraging high school students to pursue cyber security education and careers. The program brings high school students and high school teachers onto the university campus to interact with university professors and university students.

2 Background and Demographics

The summer program in cyber security builds upon an existing program for STEM high school outreach called Research Experience Vitalizing Science - University Program (REVS-UP). REVS-UP was designed from research into effective STEM outreach through hands-on experiences [1, 2, 3, 4, 5, 6, 7] and primarily focuses on more traditional science and mathematics disciplines. REVS-UP is sponsored by Chevron and it has become very popular with local high school students. In 2013, 386 students applied to approximately 100 available seats in REVS-UP.

This program augmented REVS-UP with two cyber security projects: cryptography and computer/network security. The cryptography project was led by Dr. Charles Lam in the Mathematics department. The network security project was led by Dr. Melissa Danforth in the Computer Science Department. Each project also had a CSUB student assistant who is involved in the cyber security program at CSUB.

When assigning students to REVS-UP projects, students are first assigned based on their stated preferences. If there are any seats remaining in the two cyber security projects after this initial assignment, students who have not expressed a preference and were not placed in another REVS-UP project are offered an opportunity to participate. This helps the project reach a wide range of students who might not have otherwise considered a cyber security project. Approximately half of the high school students who participated in the summer of 2013 were recruited in this fashion.

Table 1: Demographic data for participating high school students in the summer of 2013

Ethnicity	1 Decline to State	8 Asian
	1 Black/African American	3 Hispanic
	2 Two or More Races	3 White
Gender	8 Female	10 Male

8 high school students participated in the computer/network security project and 10 high school students participated in the cryptography project in summer 2013. As shown in Table 1, the demographics of the students reflect the diversity of the community in which CSUB is located. Seven local high schools were the source of students participating in the project, including three high-needs high schools.

3 Program Details

High schools students were on campus for four days each week, and attended from 9:00am to 3:00pm with a break for lunch. The time was split between lectures, worksheets, and conducting hands-on activities. REVS-UP concludes the fourth week of activities with a half-day poster competition for all participating students. The majority of the fourth week was spent preparing posters.

Students in the cryptography project were introduced to basic number theory and its use in modern-day encryption. They also learned about the history of cryptography and modern uses of cryptography. Students used a variety of hand-tracing techniques and mathematics programs such as Maple to model problems in number theory and cryptography. See Table 2 for a breakdown of the topics covered by week.

For their hands-on activities in cryptography, the students began with self exploratory worksheets on traditional substitution ciphers, the Euclidean Algorithm, modular arithmetic, the concept of inverse, Fermat's Little Theorem, and RSA encryption. This prepared them for their hands-on activities in the following three areas: factoring and its effects on RSA, elliptic curve cryptography, and zero knowledge protocols.

Students in the factoring project modeled three factorization algorithms to see the strengths and weaknesses of each algorithm. They also learned how rapid factorization would undermine the RSA algorithm. Students in the elliptic curve cryptography project learned about the foundations of the technique and how it com-

Table 2: Breakdown of general weekly activities in the two cyber security projects

	Week 1	Week 2	Week 3	Week 4
Cryptography	Simple Substitution Cipher, Polyalphabetic Substitution Cipher, Euclidean Algorithm, Modular Arithmetic, Worksheets on Topics	Fermat's Little Theorem, Modular Exponentiation Algorithm, RSA Encryption Algorithm and Proof, Worksheets on Topics	Hands-on Activities, including Programming and Experimentation	Prepare Poster on Hands-on Activities
Computer/ Network Security	Ethics and Legality, Security Concepts, Authentication Protocols, Password Hashing and Cracking, Using Linux, Hands-on Activities	Password Practices, Secure Authentication Protocols, TCP/IP Networking, Network Attacks, Social Engineering, Hands-on Activities	Malware, Access Control, Protecting Information, "Best Practices" for Security, More on Social Engineering, Hands-on Activities	Prepare Poster on Hands-on Activities, Watch Videos on Recent Security Topics (e.g. SmartTV hack, DefCon, etc.)

pares to other algorithms like RSA. Students in the zero knowledge group learned about the Fiat-Shamir protocol and its weaknesses. They also learned about the Guillon-Quisquarter protocol and how it compares to Fiat-Shamir.

Students in the computer/network security project were focused on operational security and user authentication. The students learned about traditional security principles such as confidentiality, integrity, and availability. The majority of the time was focused on user authentication, attacks against network services, attacks against stored passwords, social engineering, and malware basics. The importance of ethics in cyber security was also emphasized. See Table 2 for a week-by-week breakdown of topics.

Students in this project typically spent the morning learning about a topic collectively as a group, and then would split into smaller groups to work on their hands-on activities in the afternoon. Two hands-on projects were conducted: social engineering and using GPU rigs to crack hashed passwords.

Students in the social engineering group read portions of the book "Social Engineering" by Christopher Hadnagy, watched videos of social engineering techniques in practice, and learned about methods to counter-act common social engineering techniques. Students in the password security group used a simple GPU rig consisting of two ATI video cards to crack passwords that were hashed with several algorithms. Students used several common Linux command line tools, like sha1sum, to create their own hashed password file containing simple, medium, and secure passwords to see how long it took the rig to recover the passwords.

4 Conclusions

Student comments in a post-activity survey reflect a positive experience with most of the program. Most of the students would recommend the outreach program to their friends, and most said the program increased their interest in attending college. The primary dissatisfaction was with the REVS-UP poster competition.

5 Acknowledgments

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] P. R. Aschbacher, E. Li, et al. Is Science Me? High School Students' Identities, Participation and Aspirations in Science, Engineering, and Medicine. *Journal of Research in Science Teaching*, 47(5):564 – 582, 2010.

[2] R. L. Bell, L. M. Blair, et al. Just do it? Impact of a science apprenticeship program on high school students' understanding of the nature of science and scientific inquiry. *Journal of Research in Science Training*, 40(5):487 – 509, 2003.

[3] J. Charney, C. E. Hmelo-Silver, et al. Cognitive apprenticeship in science through immersion in laboratory practices. *International Journal of Science Education*, 29(2):195 – 213, 2007.

[4] K. Grindstaff and G. Richmond. Learners' perceptions of the role of peers in a research experience implications for the apprenticeship process, scientific inquiry, and collaborative work. *Journal of Research in Science Teaching*, 45(2):251 – 271, 2008.

[5] D. M. Hammond and M. M. Lalor. Promoting STEM careers among undergraduates through interdisciplinary engineering research. *Council on Undergraduate Research Quarterly*, 30(2):26 – 33, 2009.

[6] D. G. Markowitz. Evaluation of the long-term impact of a university high school summer science program on students' interest and perceived abilities in science. *Journal of Science Education and Technology*, 13(3):395 – 407, 2004.

[7] J. E. Stake and K. R. Mares. Evaluating the impact of science-enrichment programs on adolescents' science motivation and confidence: The splashdown effect. *Journal of Research in Science Teaching*, 42(4):359 – 375, 2005.