Building a Cryptography Rotation Pipeline Intervention for Cyber Athletes: Curriculum Design and Coaching Lessons Learned

Suzanna Schmeelk[1] and Tom McGuire[2]
[1]St. John's University, Queens, New York, USA
[2]John's Hopkins University, Maryland, USA

***Abstract*—The United States Cyber Games started in 2021 to compete internationally in the annual International Cyber Competition (ICC). The United States Team prepares a seasonal team based on yearlong, volunteer coaches, volunteer athletes, and a rigorous virtual national training program to prepare cyber athletes to compete. Historically, the ICC has aimed to attract early-career professionals and raise global awareness of the education and skills needed in the area of cybersecurity. Teams from around the globe come together annually to compete in the ICC. Each year the areas of focus are updated and in general include: web application and system exploitation, cryptography, reverse engineering, hardware challenges, and attack/defense challenges.**

Early in the development of the first US team preparation to participate in their first ICC, it was realized a need to create a pipeline program to prepare strong athletes for potential entrance onto a future team if they were not already on the current team. This research reports on the volunteer pipeline coaching for building the curriculum, assessment challenges, and voluntary Institutional Review Board approved athlete feedback from the cryptography (crypto) training sessions of Season II in the US Cyber Games pipeline program. The crypto rotation is one of at least five rotations in the pipeline program where each rotation lasts a month on average.

This full paper reports on our volunteer coaching insights, feedback, and curriculum for the crypto rotation sessions for need to know crypto topics for likely capture the flag and attack/defend competition questions and exercises including: symmetric, asymmetric, weak modes, padding schemas, key concepts, certificates, pseudo random number generators (PRNG), PRNG weaknesses, general crypto CTF tooling, socat usage, pcap extraction/interpretation related to RSA, Python related cryptography tools, Transport Layer Security (TLS) vulnerabilities, TLS packet exchange, and other cryptographic concepts, Given a research literature gap on building such a volunteer national team to compete international, we also report on the coaching experiences, challenges topics created for the rotation as well as the importance of proper tooling and preparation for the athletes. We share international topics advised for coverage for ICC training competitions. And, then report on coaching feedback and student voluntary IRB-approved feedback. Lastly, we share coach and athlete feedback and insights for next iterations of building a similar training session.

***Index Terms*—Cybersecurity Gamification, Cryptography, Capture the Flag, Jeopardy, Athlete Training**

I. Introduction

Cybersecurity is critical to the safely of our digital infrastructure and international citizens. The International Cybersecurity Competition has been hosted by the European Union for many years. In 2022, the United States joined the competition with a national team. The annual event provides international communication and skills building which may play a role in serious future cyber concerns.

The team for Season I and Season II were comprised of volunteer coaches and volunteer athletes (under their mid-20s age) from across the United States [7]–[9]. Early it was recognized a need to create a pipeline program to help ready strong athletes for a future year especially if they did not make the current year team seat. The training programs areas of focus are continuously improved but in general include: web application and system exploitation, cryptography, reverse engineering, hardware challenges, and attack/defense challenges. On average each rotation each rotation lasts a month. This paper reports on building, coaching, feedback, and lessons learned for building the first crypto rotation in Season II of the pipeline accelerated program.

II. Literature Review

Literature exists for building capture-the-flag experiences as well as building cryptography curriculum in K-12, undergraduate, and graduate programs. Little literature, however, exists on building curricula and coaching (either national or international) for capture-the-flag training programs highlighting specific cryptography training which will be the focus of the next sections of our research.

Beltrán, Calvo, and González [1] summarize their experiences introducing gamification in Computer Security labs through on-line Capture The Flag competitions, trying to improve the engagement of our students and to improve their reverse engineering, vulnerability exploitation, cryptography and secure programming skills. The authors report on the learning outcomes, design, setup and implementation of the gamified labs. Results from these first experiences show that students perceive the new labs design as more interactive, collaborative, useful and motivating compared to the previous approach based on individual virtualized exercises. All this minimizing administrative, financial and technical costs through the use of the open and free Facebook Capture The Flag platform.

Matias et al., [2] propose NIZKCTF as a first open-audit CTF platform based on noninteractive zero-knowledge proofs. Their work springs from the Brazilian cybersecurity community.

Ford et al., [3] developed the CTF Unplugged project, as inspired by the CS Unplugged project, with a primary goal to teach students with little or no technical cybersecurity knowledge without the direct use of technology. The main leanings for students participating in the project were to gain insights into skills of working cybersecurity professionals and cyber-career centric problem-solving skills. The authors report on insights from introducing 36 high school students participating in the Tennessee Tech University GenCyber Camp. Findings suggest that students gain in knowledge, confidence, and comfort level after participation.

Leune and Petrilli [4] report on incorporating Capture-The-Flag (CTF) sessions gamified simulations of cybersecurity breach scenarios. Their findings suggest that the experiences improves student confidence based on surveys pre/post CTF surveys in an undergraduate cybersecurity class.

Venkatagiri et al., [5] report on a four-month-long Research through Design process to design and evaluate a novel interaction style called collaborative capture the flag competitions (CoCTFs) through CoSINT. CoSINT is a platform that enables a trained crowd to work with professional investigators to identify and investigate social media misinformation. Their mixed-methods evaluation of CoSINT suggest that the platform enhances communication between participating members to quickly identify and debunk misinformation. The authors discuss tool implications and CTF investigation designs.

Vykopal, Švábenský, and Chang [6] report on their experience from using jeopardy CTF games as homework assignments in an introductory undergraduate course. Their analysis revealed four important CTF game building aspects: scoring, scaffolding, plagiarism, and learning analytics. The authors share reccomendations and feedback from their experiences.

O'Connor et al. (2023) [7], [8] and Jackson and Payne [9] report on volunteer coaching of the first ever U.S. Cyber Games Season I to participate in International Cybersecurity Competition in Athens, Greece. The authors provide feedback on building different aspects of the training program.

Deeb and Hickey [10] reports on a pilot study of a 3D game that was designed to teach students introductory concepts in security and cryptography version of the "Escape the Room." The game includes puzzles where the player needs to find and solve a sequence of problems to escape from a room. The game was tested with a group of 16 students, and pre/post test surveys were collected and included participant understanding of certain cryptography concepts.

Rayavaram et al., [11] reported on the design and development of a simple, visual, and narrative K-12 cybersecurity curriculum. The curriculum leverages the Scratch programming platform to demonstrate and teach fundamental cybersecurity. They evaluate the student's comprehension of the introduced concepts from surveys.

In terms of course development, Al-Hamdani [12] reports on missing factors in cryptography algorithms curriculum designed to teach information security. Uskov [13] report on cryptography courses a Bradley University based on most recent ACM/IEEE guidelines and focused on practitioner's approach in teaching.

III. Topic Coverage

The curriculum for the crypto pipeline rotation sessions involved a need to know of foundational topics for likely capture the flag and attack/defend competition questions. The coaching curricula, walk-throughs, and athlete challenges are discussed discussed in the next section. This section describe high-level concepts that were incorporated into the curricula.

A. Public and Secret Key Encryption

Using best practice cryptographic techniques for public and secret key encryption is essential for CTF competitions. Topics include weak construction modes, encryption algorithm rounds, initialalization vectors, pseudo-random number generator (PRNG), padding schemes, and key management concepts.

B. Key Exchange Protocols and PKI

The Public Key Infrastructure, key negotiation, and certificate distributions are a means of public key distribution and validation across the internet. A common encoding scheme is X.509 certificates in Base64 and commonly saved in a file with PEM extension (Privacy Enhanced Mail). PME files can be employed by tools such as *openssl* to decode it.

C. TLS and Data in Transfer

Transport Layer Security (TLS) is a protocol that provides a secure channel between two communicating applications. TLS evolved from earlier predecessor variations of the Secure Socket Layer (SSL). It is designed to run on top of TCP but can be implemented with other protocols. Client programs, such as browsers, need to load a list of trusted certifying authority (CA) certificated beforehand, or they will not be able to verify any certificate. If the signing CA is on the list, the certificate can be directly verified. Session keys are then negotiated between the client and server applications for the transfer of more data. The communication is bi-directional so both directions use separate keys. Athlete Understanding of detailed aspects of the TLS protocol includes examining network traffic and understanding weaknesses at different points in the handshake and session.

D. Password Generation, Storage, and Cracking

Cryptography secure password generation and storage is essential for maintaining the integrity of authentication. Our United States National Institute of Standards and Technology (NIST) provides guidance (e.g. 800-63B) on best practices including secure generation functions, hashing rounds, salting, and storage. Understanding weaknesses in the storage and management lead to understanding how to crack insecure techniques.

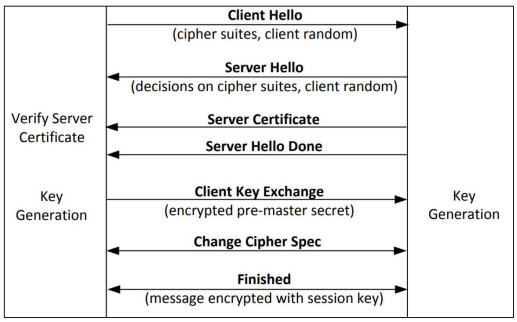

Fig. 1. TLS Handshake Protocol.

E. CTF Tooling and Python Packages

There are many tools useful for solving crypto related CTF challenges. Building athlete research skills is foundational to finding different tools to solve different problems. For example, *socat* is a command line based utility that establishes two bidirectional byte streams and transfers data between them. In python, there are many python related packages such as *pwn* that provide useful and robust tooling.

F. Other cryptographic concepts

Other related cryptography concepts include stenography where information is hidden in an ordinary file to avoid detection. Stenography can be coupled with cryptography to add complexity to challenges. Some CTFs are air gaped meaning that athletes do not have internet access while working on challenges so athletes must properly prepare in advance for different challenge scenarios.

G. Debunking Cryptographic 'Fake News' Concepts

There are many common myths about cryptography that show up in industry, academics, and CTFs. A main confusion is between encoding and encryption where cryptography is a main differentiating factor. Other myths include believing cryptography lasts forever and not properly understanding the deprecation process. The depreciation process especially of cryptographic algorithms elements. When cryptography is not properly implemented or entirely missing, it is essential to know where to look for for basic patterns–especially when crypto is missing or not implemented properly. For examples, improper key storage can occur when the developer writes the key out in plain text and appends to beginning or end of the protected file. In such a case, inspecting the raw file bytes may expose keys or passwords.

IV. Crypto Practice Challenges

Each year the areas of focus for the US Cyber Games athlete pipeline program are updated and in general include: web application and system exploitation; cryptography; reverse engineering; hardware; and attack/defense topics and challenges. Each rotation is approximately a month starting with the first of the year. Therefore, the crypto rotation encompassed a month-long activities. The overall design was to to introduce concepts and encourage the athletes to train on the challenges. The challenges were distributed after each of the two coach-led sessions of lectures with walk-throughs. Given the volunteer nature of the pipeline athlete participants, solving the challenges were optional as dependent on pipeline athlete time constraints. After giving live online national team coaching sessions at timeframes that generally worked nationally. The coach recordings and challenges were hosted up on on the team pipeline learning management system (LMS). The athletes could work on the rotation lessons anytime before the Season II ended and would upload their results to the shared team LMS. The coaches and program directors could review athlete progress.

1) Crypto Session 1, Week 1-2: The first session encompassed a week of training and a second week of solving challenges. The first session was designed to introduce athletes to cryptographic concepts likely found on CTFs and popular python modules for CTFs. The session coaches walked-through an exercise of Elliptic Curve Digital Signature Algorithm (ECDSA) Nonce Reuse, an Oracle Padding challenge, and example of solving Steganography (steg). (In CTF challenges, steg techniques can fall into digital forensics challenges and can also be coupled with cryptography to increase difficulty.) After the lecture, the coaches released exercise for practice. The athletes managed their work in the LMS where they could follow-up and post questions. The coaches provided resources for the athletes both during the live office hours and as follow-up asynchronous questions.

Lecture walk-through 1 In the first walk-though the coaches showcased a Cipher Block Chaining (CBC) challenge showing the athlete how to use a python program to decrypt the challenge flag by manipulating where the flag appears in the decryption process.

Lecture walk-through 2 In this walk-though the coaches showcased a ECDSA challenge in which the nonce is reused allowing us to recover the secret and decrypt the flag.

Lecture walk-through 3 STEG - In this walk-tough the coaches showcased a simple steg challenge and showed athletes how to utilize CyberChef to help decode the flag.

Athlete Exercise 0 The first exercise was designed to increase athletes understanding of using Python to solve challenges. In the challenge, the athletes use pwntools to interact with a number guessing game. The sample code is below:

```
from pwn import *
import sys
import argparse

def solveit( ip, port ):
with context.local(log_level='INFO'):
with remote(ip, port) as target:
    def getinitialline():
          # Think about what you want to
          # receive up until here..
          # This is your first interaction
          # with the process..
```

```
        _ = target.recvuntil(b'SOMETHING HERE')
        return

    def submitpass(ct):
        # We want to send the text as bytes
        # (this is the encode utf-8)
        target.sendline(ct.encode('utf-8'))
        # Do you want to wait again here?
        # If so, what would you like to
        # wait for?
        return

    def submitguess(ct):
        # What should this entail?
        # Do you want to wait again here?
        # If so, what would you like to
        # wait for?
        return

    success = -1
    print('Getting initial line')
    getinitialline()
    submitpass('SOMETHINGHERE')

    # Guess a random number (you could
    # also guess the same number each
    # interaction..but try
    # changing it up)

    ret = submitguess('SOMETHINGHERE')

    # Check to see if your guess is
    # correct
    return success

def main():
    """Main entry point"""
    parser = argparse.ArgumentParser(
        description='Client for helping
        connect to a service and
        interact'
    )
    parser.add_argument(
        '-i', '--ip',
        default='127.0.0.1',
        required=False,
        help='The IP to connect to '
    )
    parser.add_argument(
        '-p',  '--port',
        default=9999,
        type=lambda x: int(x,0),
        required=False,
        help='The port to connect to '
    )
    args = parser.parse_args()
    # Setup a simple while loop here to
    # keep trying.  You could also
    # include your guess as an argument
    # as well keep track of the number
    # of tries and at the end print the
    # number of tries and the guess
    # that was successful

if __name__ == '__main__':

    main()
```

Athlete Exercise 1 The first exercise was designed to have athletes practice breaking a small RSA modulus similar to the one provided in the lecture. The athletes were given an RSA public key (mypubkey.pem) and expected to find a way to decrypt the flag.enc file and capture the flag. The flag was encoded to further increase the difficulty of the problem however a flag pattern hint was given.

Athlete Exercise 2 The second exercise was designed to have the athletes practice with steg. In the challenge athletes were given an image file and are asked to find a hidden message within. The flag pattern hint was also given.

Athlete Exercise 3 The third exercise was designed to have the athletes practice with the Chinese Remainder Theorem. In the challenge, the athletes are given an the encryption exponent used by three parties and was also seen by the attacker. The athletes are asked to recover the sent messages Without factoring the moduli, recovering the decryption exponent or performing a brute force attack.

Athlete Exercise 4 - The fourth exercise was designed to have the athletes practice analyzing a PRNG. In the exercise, athletes were given a PRNG system in which they could interact; they were asked to recover the seed for these systems and ultimately provide correct guesses for the next values.

2) Crypto Session 2, Week 3-4: The second session encompassed the second-part of the month with a week spent training and a second week of solving challenges. The session included foundational topics not fully discussed in Session 1: hashing and data-in-transfer. The focus on password Storage methodologies included password cracking concepts and tools. The first two coach walk-throughs examined password cracking. The session also covered the public key infrastructure (PKI), transport layer security (TLS), and well documented ways to break PKI/TLS. The second two walk-throughs included using Wireshark to examine the TLS handshake and use of SSLLabs to analyze a website. The end of the session was focused on debunking fake crypto news which are common mistakes and myths about crypto.

Lecture walk-through 1 The first demo involved showcasing password cracking tools with the KoreLogic DEFCON Crack Me If You Can [14] challenges shown in Figure 3. The coaches build and showcased the module up in the Amazon Web Service (AWS) cloud.

Lecture walk-through 2 In the second walk-through the

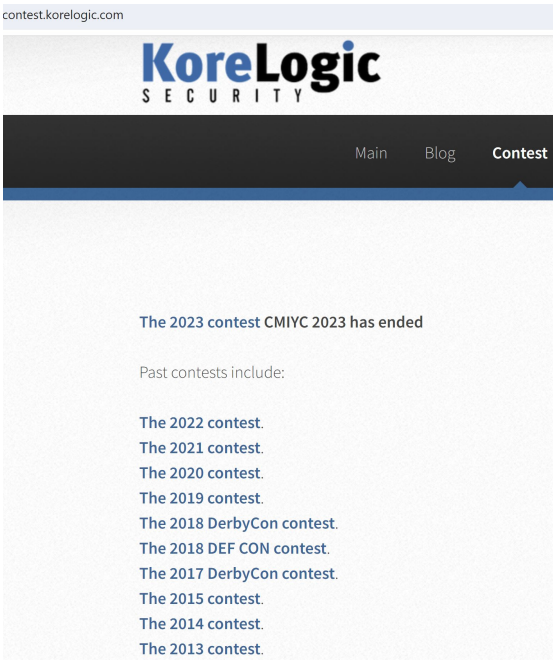

Fig. 2. KoreLogic Challenges Sets by Year [14].

Fig. 3. KoreLogic Challenges Set for 2012 [14].

coaches showcased and encouraged the athlete to complete breaking password protected files from the KoreLogic DEFCON Crack Me if You Can challenges.

Lecture walk-through 3 In the third walk-through the coaches showcased how to capture the TLS handshake with Wireshark. The coaches also showcased how to decryp encrypted traffic once the encryption keys are known.

Lecture walk-through 4 In the final demo the coaches walked-through the use of SSLabs to analyze a web server TLS negotiation traffic. The coaches then explained the findings and discussed how the analysis works.

Athlete Exercise 0 In this exercise the coaches encouraged the athlete to complete the early KoreLogic DEFCON Crack Me if You Can password protected files (e.g. zip, pdfs, docs, etc.) as the earlier crypto challenges from 10 years ago (e.g. 2012) are easier to break as most of the cryptography has become deprecated from weaknesses. Once (or if) the athletes could solve the earlier challenges, they were encouraged to move to more recent challenges with stronger implemented cryptography.

Athlete Exercise 1 In this exercises the coaches encouraged the athlete to complete the earlier KoreLogic DEFCON Crack Me if You Can password files of hashes as again the earlier crypto challenges from years ago are easier to break. Once (or if) the athletes could solve the earlier challenges, they were encouraged to move to more recent challenges with stronger implemented cryptography.

Athlete Exercise 2+ In this exercises the coaches encouraged the athletes to identify the components of the TLS handshake via wireshark, practice decryption traffic once given the proper keys, and scan web-servers to identify common weaknesses via SSLLabs.

V. International Suggested Topic Coverage

The European Cyber Security Challenge (ECSC) [21] advises an annual curricula of training topic coverage. General advise for preparation at international training competitions was quite broad in topics. We reviewed the guidance given and summarize different cryptography-related topics to the athletes. Our guidance was also shared with the travel team. The summary is presented in the following subsections.

A. ECSC Curricula: Cryptography General

Given that cryptography is fundamental to information security, core cryptography concepts are highlighted in the curricula as fundamental knowledge. Guidance for attendants to be familiar with cryptographic primitives, their protocols, their usage, and their weaknesses [15].

B. ECSC Curricula: Confidentiality/encryption

CTF topics important for the confidentiality and encryption of information and communications include the following:

- Symmetric-key encryption and public-key encryption
- Strong encryption and weak encryption, key length and exhaustive key search, Moore's law
- Stream ciphers, one-time pad, LFSR-based stream ciphers, E0, SNOW-3G, RC4
- Blockciphers, DES, 3-DES, AES
- Blockcipher modes of operation for encryption: CBC, CTR, OFB, security bound for CBC
- One-way functions, Diffie-Hellman, ElGamal encryption, trapdoor oneway functions, RSA
- Hybrid encryption, KEM-DEM, PKCS standards

C. ECSC Curricula:Integrity/data authentication

- Data authentication versus encryption

- Symmetric-key data authentication (MACs) and public-key data authentication, non-repudiation
- Hash functions: SHA-1, SHA-256, SHA-512, SHA-3
- Collisions, preimages, birthday paradox, exploiting a collision to forge signed code
- Blockcipher mode of operation for authentication: CBC-MAC, CMAC
- Blockcipher mode of operation for authenticated encryption: GCM, CCM, OCB
- Data authentication algorithm based on hash function: HMAC
- One-time MACs: PMAC, Poly1305
- Digital-signature algorithms: RSA, ElGamal, DSA, ECDSA
- Signatures with message recovery, signatures with appendix, encoding, PKCS standards

D. ECSC Curricula: Identification/entity authentication

- Passwords, password quality, password storage, PAKE
- Challenge-response by means of MAC, by means of digital signature, reflection attack
- Authenticated key agreement

E. ECSC Curricula: Key agreement

- Nonces, replay, timeliness
- Session keys, forward secrecy
- Trusted Third Parties
- Kerberos
- Diffie-Hellman, person-in-the-middle attack, key authentication
- STS/IKE

F. ECSC Curricula: PKI Fundamentals and In Practice

The distribution of credentials represents a special problem in itself, as identification and trust on the Web are hard to establish and initialize. It is still necessary to know who owns certain public key pairs and certificates, and in this respect different Public Key Infrastructures have been developed and partially deployed. The teams of ECSC should have profound understanding of such technologies.

- Communicating by using PGP, GPG or similar, keychain, trust in a key-pair
- Certificates, root certificates, trusted CAs, self-signed certificates, certificate chain, parsing of X.509, revoking, CRLs, OCSP, timestamping

G. ECSC Curricula: Cryptanalysis

A good survey on modern cryptanalysis techniques can be found in the overview of the external analysis on Simon and Speck [16]. An in-depth treatment of block ciphers, differential cryptanalysis and linear cryptanalysis can be found in [17].

H. ECSC Curricula: Networking + Security in-Practice

The connectivity of the devices has led to a large attack surface. This is the case both for the devices, which are suddenly globally reachable, but also for the network infrastructure itself. The teams, hence, have to understand the Internet architecture and basic protocols, as well as the basic security assumptions, threats, and protocols that are commonly used today. Suggested references to be familiar with are Townsend et al. [18] *Getting staTools and techniques for lowpower networking*, Rossberg and Schaefer's [20] *Security in Fixed and Wireless Networks*, and Padgette et al., [19] *Guide to Bluetooth Security*. Relevant cryptography related items or items that may rely on cryptographic ideas are as follows:

- Internet architecture and protocols
- Layered model: ISO/OSI, TCP/IP
- Basic application layer protocols: HTTP, FTP, SSH
- Common threats: Eavesdropping, Masquerade, Modification/Loss of information, Forgery, Authorization violation, Sabotage (Denial of Service), Repudiation
- Dolev-Yao adversary, Sniffing, MitM, Spoofing, Distributed attacks, Reflection and Amplification
- Link layer security: 802.1X, PPP, CHAP, PPTP, WEP/WPA, MAC-sec
- IPsec
- Transport layer security: TLS, SSH
- Infrastructure security: BGPsec, EDNS, DNS Cookies, DNSSEC
- Bluetooth (incl. BLE) security
- RFID and NFC security
- Wireless network security: ZigBee, Z-Wave, Wi-Fi, LP-WAN, NB-IoT
- Network administration and security: promiscuous mode, ad-hoc networking, mesh networking, identity management, encryption, authentication, authorization

VI. Coach Lessons Learned and Athlete Feedback

As two volunteer coaches for the U.S. Cyber Team Pipeline Program comprised of volunteer pipeline athletes, the month-long cryptography rotation we built and ran was overall a success. We as coaches learned and shared a great deal with the United States Team. Overall, the pipeline athletes whom attended our sessions expressed that they learned a lot from the rotation. The atheltes also left positive feedback for the coaches in the LMS. Athletes agreed to participate in our IRB approved survey however, gave little feedback to incorporate on improving the sessions for the next iteration.

The lessons and walk-through were given online during Eastern time late evening times (to include live coverage across the different United States timezones) with asynchronous communications in Discord and the team shared LMS. The lessons and challenges were managed through the Google Learning Management System. Coaches provided office hours during their rotations to answer questions. Overall, the collaboration and planning took months of preparations given all the different stakeholder needs to be addressed.

Given the lack of ready curricula, we developed the sessions based on our industry experience and own CTF experiences. Going forward it could be useful to build ontologies for learning concepts to unify topics and clarify gaps in understandings and curricula.

A. Conclusions and Future Work

This research reports on building and coaching a cryptography rotation for the pipeline program of the U.S. Cyber Games Season II. In 2022, the United States participated in their first International Cybersecurity Competition (ICC) in Athens Greece [7]. From Season I, the second season, Season II, started with a stronger pipeline training program.

This research focuses on building the curricula and coaching the sessions for one rotation of the pipeline training program, the crypto rotation. We report on coaching the rotations, lessons planned, challenges formulated, lessons learned, feedback gleaned, and future suggestions. Cryptography underlies many, if not all, cybersecurity elements. It has historically been taught from a non capture the flag (CTF) environment perspective. This research fills the gap on building such a curricula to educate the next generation of world class athletes.

REFERENCES

[1] M. Beltrán, M. Calvo and S. González, "Experiences Using Capture The Flag Competitions to Introduce Gamification in Undergraduate Computer Security Labs," 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2018, pp. 574-579, doi: 10.1109/CSCI46756.2018.00116.

[2] P. Matias, P. Barbosa, T. N. C. Cardoso, D. M. Campos and D. F. Aranha, "NIZKCTF: A Noninteractive Zero-Knowledge Capture-the-Flag Platform," in IEEE Security & Privacy, vol. 16, no. 6, pp. 42-51, Nov.-Dec. 2018, doi: 10.1109/MSEC.2018.2875324.

[3] Vitaly Ford, Ambareen Siraj, Ada Haynes, and Eric Brown. 2017. Capture the Flag Unplugged: an Offline Cyber Competition. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17). Association for Computing Machinery, New York, NY, USA, 225–230. https://doi.org/10.1145/3017680.3017783

[4] Kees Leune and Salvatore J. Petrilli. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17). Association for Computing Machinery, New York, NY, USA, 47–52. https://doi.org/10.1145/3125659.3125686

[5] Sukrit Venkatagiri, Anirban Mukhopadhyay, David Hicks, Aaron Brantly, and Kurt Luther. 2023. CoSINT: Designing a Collaborative Capture the Flag Competition to Investigate Misinformation. In Proceedings of the 2023 ACM Designing Interactive Systems Conference (DIS '23). Association for Computing Machinery, New York, NY, USA, 2551–2572. https://doi.org/10.1145/3563657.3595997

[6] Jan Vykopal, Valdemar Švábenský, and Ee-Chien Chang. 2020. Benefits and Pitfalls of Using Capture the Flag Games in University Courses. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, 752–758. https://doi.org/10.1145/3328778.3366893

[7] O'Connor, T. J., Brown, D,, Jackson, J., Payne, B., and Schmeelk, S. (2023) Compete to Learn: Toward Cybersecurity as a Sport. Journal of Cybersecurity Education, Research and Practice, v2023 n1 Article 6

[8] O'Connor, T. J., Brown, D,, and Schmeelk, S. (2022) Going for the Gold! Insights and Lessons Learned from Coaching the First-ever US Cyber Games Team. Presentation at the 2022 NICE Conference and Expo, Atlanta, Georgia. Retrieved from: https://www.nist.gov/news-events/news/2022/03/registration-open-2022-nice-conference-expo-atlanta-georgia

[9] Jackson, J. and Payne, B. (2022) Accelerating To Victory! Leveling The Playfield in Information Security Through an Accelerated Training Program. Presentation at the 2022 NICE Conference and Expo, Atlanta, Georgia. Retrieved from: https://niceconference.org/wp-content/uploads/2022/06/NICE-Breakout-2-Day-2-Chastain-D.E..pdf

[10] F. A. Deeb and T. J. Hickey, "Teaching Introductory Cryptography using a 3D Escape-the-Room Game," 2019 IEEE Frontiers in Education Conference (FIE), Covington, KY, USA, 2019, pp. 1-6, doi: 10.1109/FIE43999.2019.9028549.

[11] P. Rayavaram et al., "Designing a Visual Cryptography Curriculum for K-12 Education," 2023 IEEE Global Engineering Education Conference (EDUCON), Kuwait, Kuwait, 2023, pp. 1-10, doi: 10.1109/EDUCON54358.2023.10125191.

[12] Wasim A. Al-Hamdani. 2009. Missing factors in teaching cryptography algorithms for information security tracks. In 2009 Information Security Curriculum Development Conference (InfoSecCD '09). Association for Computing Machinery, New York, NY, USA, 15–20. https://doi.org/10.1145/1940976.1940982

[13] A. V. Uskov, "Applied Cryptography for Computer Science programs: A practitioner's approach," 2013 3rd Interdisciplinary Engineering Design Education Conference, Santa Clara, CA, USA, 2013, pp. 63-70, doi: 10.1109/IEDEC.2013.6526762.

[14] Korelogic (n.d.) Crypto Challenges. https://contest.korelogic.com/

[15] Lars R. Knudsen. Cryptology, how to crack it.

[16] Ray Beaulieu et al. Notes on the design and analysis of SIMON and SPECK. Cryptology ePrint Archive, Report 2017/560. http://eprint.iacr.org/2017/560. 2017.

[17] Lars R. Knudsen and Matthew J.B. Robshaw. The Block Cipher Companion. 2011.

[18] Kevin Townsend, Carles Cuf´ı, Robert Davidson, et al. Getting staTools and techniques for lowpower networking." O'Reilly Media, Inc.", 2014.

[19] John Padgette et al. "Guide to Bluetooth Security". In: Special Publication (NIST SP)-800-121 Rev 2 (2017).

[20] Michael Rossberg and Guenther Schaefer. Security in Fixed and Wireless Networks. Wiley, 2016.

[21] European Cybersecurity challenge Curricula (n.d.) https://ecsc.eu/about/ecsccurricula.pdf/view