Tutorial: Parry and RIPOSTE: Honing Cybersecurity Skills with Challenge-Based Exercises

Fabian Monrose and Jan Werner
University of North Carolina at Chapel Hill

Summary

Although cyberspace has transformed the way we live our lives, many well-known vulnerabilities in critical infrastructure have gone unchecked, and the reliance on technology has left us increasingly at risk. Today, cybersecurity attacks and breaches are an all too familiar event, underscoring the need for establishing a front line defense to significantly bolster the security and resilience of cyberspace against skilled adversaries. However, even after repeated calls to action for building a highly capable cybersecurity workforce, we still lack enough skilled professionals to help defend our nation against a myriad of known systemic risks.

Objectives: While there have been numerous attempts over the past decade to address the dearth of talent and foster greater capacity building in cybersecurity, it is only recently that stake-holders in government, industry, and academia have started to get more involved [1]. For sure, meeting the challenges of training the next generation of cybersecurity professionals in a discipline that changes rapidly is not easy, and success in that endeavor mandates a hands-on approach to educating those interested in careers in cybersecurity. Moreover, in order to build a capable work force it is imperative that folks with a passion for programming have access to environments that support learning and testing of weaknesses in software at the application and operating system levels. Unfortunately that is rarely the case today, and we may be losing many talented individuals early on as they choose career paths because either systems-oriented material is not presented to them in an appealing or engaging way [2, 3], or the resources needed to explore the subject are not readily accessible. Indeed, if one is not already working as a cybersecurity practitioner there are surprisingly few opportunities to learn the prerequisite skills for becoming a good security professional. Manson and Pike [2] may have put it best: "*education a cybersecurity professional is similar to training a pilot, an athlete or a doctor. Time spent on the task for which the person is being prepared [for] is critical for success.*" For example, while the problems brought on by memory errors can easily be taught in a way that students are book-smart about the issues, effectively learning how to spot such problems, exploit them, and design defenses that thwart specific classes of attacks only sink in once the learners have had time to attempt these tasks on their own. Thus, to have any chance of building a diverse pool of cybersecurity professionals we must be more aggressive in providing interested persons with better — and more accessible — options for attaining the necessary skills.

Learning outcomes: We will use the IEEE-supported `Riposte`[1] framework to provide learners with an introduction to protocol reverse engineering and cryptanalysis via a series of challenged-based exercise, disguised as a 2D top-down shooter game.

A. Tutorial Description

Student-centered learning, and in particular, *challenge based learning* (CBL) — which encourages students to use their knowledge and technology to solve real-world problems — is known to be very effective[2]. In such tasks, learners are challenged to draw on prior learning, acquire new knowledge, work as a team, and use their creativity to arrive at solutions given as part of an active learning exercise. Active learning exercises can be thought of as anything that all learners in a class are called upon to do other than simply listening to a lecture and taking notes. Typically, learners participate in some form of competition, and as such, learning accelerates because participants are often highly motivated by some goal (*e.g.,* staying upon a leader board and potentially winning a prize).

Our experience shows that while challenge-based learning usually improves overall learning, its benefit vary from one student to the next, based on interests and motivation. That is, its success depends *heavily on how interesting the exercises are* — which directly impacts the level of self-study, peer instruction, and overall en-

[1] In fencing, the "riposte" is an offensive action made by a fencer who has just parried an attack.

[2] See O'Neil and McMahon, *"Student-Centered Learning: What does it mean for students and lecturers."*

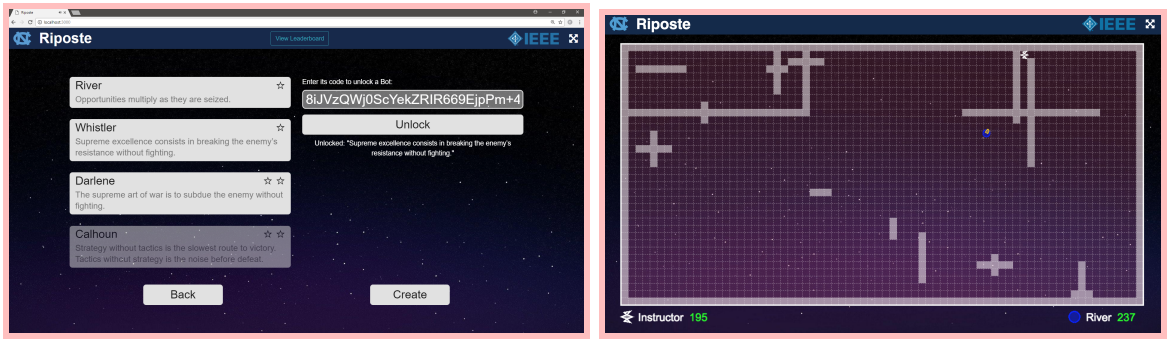

Fig. 1. Interface for Game View; Playground for Protocol Reverse Engineering and CBC-bit Flipping Exercises

gagement. And, for students to become lifelong learners, it is iterative that they take responsibility for their own professional development beyond the classroom. This is especially true for the fast moving field of cybersecurity. Thus, motivating students to learn on their own plays in important part in capacity building. Toward that goal, we will expose learners to `Riposte`, which forces students to explore creative applications of what they know as a means to solving a semi-structured problem.

What the Tutorial Covers

- Format: Mini-presentations intermixed with active learning exercises. We expect several short exercises that build upon each other.
- Learning outcomes: Introduction to traffic analysis, protocol reverse engineering, and (time-permitting) directed cryptanalysis.

We expect the tutorial will span two 90 min blocks. In the first block, learners will improve their traffic analysis skills, and then work independently or in small groups to defeat adversaries that do not abide to the rules of engagement. In the second block, learners will use cryptanalysis to unlock new game bots, and then will join ranks to neutralize or defeat colluding adversaries. Exercises include:

1) Getting Your Feet Wet: Observing & Modifying Network Traffic in the Browser.
2) Protocol Reverse Engineering Made Easy, Javascript Edition.
3) The Best Defense is a Strong Offense: Hacking the Game Client.
4) Moving On Up: Bit Flipping for Fun and Points.
5) Zone Defense: Confining More Advanced, Colluding, Adversaries.

Each block would be capped at 25 persons.

About the Instructors

The tutorial will be co-led by Fabian Monrose and Jan Werner. **Fabian Monrose** is a Professor at the University of North Carolina at Chapel Hill (UNC-CH). His research interests are in all aspects of systems security, and has published extensively in flagship security venues. He has also been the recipient of several best paper awards and won a teaching award by the undergrads for his course on *Introduction to Computer Security*, which offers several challenge-based learning exercises. **Jan Werner** is a research staff member at UNC-CH. His interests are in systems-oriented aspects of computer security, with particular expertise in secure software engineering practices, operational security, and security of embedded systems. He has co-taught the *Introduction to Computer Security* course with Professor Monrose. In 2015, he was recognized for his outstanding teaching service.

References

[1] M. Kwon, M. J. Jacobs, D. Cullinane, C. G. Ipsen, and J. Foley. Educating cyber professionals: A view from academia, the private sector, and government. *IEEE Security Privacy*, 10(2):50–53, March 2012.
[2] Daniel Manson and Ronald Pike. The case for depth in cybersecurity education. *ACM Inroads*, 5(1):47–52, March 2014.
[3] Sheila Tobias. *They're Not Dumb, They're Different: Stalking the Second Tier (Occasional Paper on Neglected Problems in Science Education)*. Research Corporation, 1990.