2016

Talking about Talking about Cybersecurity Games

Gondree, Mark

;login: Spring 2016 VOL. 41, NO. 1. p. 36-39
http://hdl.handle.net/10945/50282

Talking about Talking about Cybersecurity Games

MARK GONDREE, ZACHARY N J PETERSON, AND PORTIA PUSEY

Mark Gondree is a security researcher with an interest in cybersecurity games for education and outreach. With Zachary Peterson, he co-founded 3GSE, a USENIX workshop dedicated to the use of games for security education, and released [d0x3d!], a board game about network security to promote interest and literacy in security topics among young audiences. Gondree is a Research Professor at the Naval Postgraduate School in Monterey, CA. gondree@gmail.com

Zachary Peterson is an Assistant Professor of Computer Science at Cal Poly, San Luis Obispo. He has a passion for creating new ways of engaging students of all ages in computer security, especially through the use of games and play. He has co-created numerous non-digital security games, including [d0x3d!], a network security board game, and is co-founder of 3GSE, a USENIX workshop dedicated to the use of games for security education. znjp@calpoly.edu

The recent explosion of cybersecurity games not only reflects a growing interest in the discipline broadly, but a recognition that these types of games can be entertaining as well as useful tools for outreach and education. However, cybersecurity game terminology—those terms used to describe or communicate a game's format, goals, and intended audience—can be confusing or, at worst, misleading. The result being a potential to disappoint some players, or worse, misrepresent the discipline and discourage the same populations we intend to attract. The year 2015 marked the second USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE), co-located again with the USENIX Security Symposium. At the event, we invited a community conversation about terminology for cybersecurity games. The conversation was the seed of a draft vocabulary report to be presented to the Cybersecurity Competition Federation for comment and possible adoption. In this article, we summarize some of the issues arising from that discussion.

Cybersecurity competitions are growing in both popularity and diversity. The Web site CTFtime [1] reports that there have been an average of 56 events per year since 2013; this is over one game every week. The International Capture the Flag (iCTF) competition has seen participation steadily increase, with the past five years averaging more than double the participation seen in prior years. There are at least three separate US leagues where bracketed, regional play culminates in a national competition. DARPA's Cyber Grand Challenge is the latest variation; it is "research in CTF form." During DEFCON 2016, participants will engage in a technology demonstration in a game format. In the midst of this cybersecurity game renaissance, we see designers, organizers, and researchers facing a semantic gap when describing and discussing cyber competitions.

Some terms used to describe cybersecurity games are based on analogy, sometimes stretched to where the relationship becomes weak: capture the flag (CTF), *Jeopardy*-style, quiz bowl, etc. Other terminology is invented but without wide adoption and therefore still evolving in meaning: e.g., hack-quest, inherit-and-defend, hack-a-thon. Certainly, game format can be a deciding factor for players, who may be unable to participate in person for non-virtual events, may be unable to assemble a group for team play, or may be unavailable to engage in a full-day, synchronous competition. Thus, at the very least, a common lexicon would help players and teams to identify competitions aligned with their interests and abilities.

Generating such a lexicon is non-trivial, however, as players come to games from different backgrounds, with various motivations and desired outcomes [3]. Players may be novice learners seeking to build new skills or practice learned skills. These players may only want to play if they know solutions or write-ups will be released after the event. Others may want challenges to persist after the competition, allowing players to complete them outside the competition or present their solutions to a class or study group. Experts may want harder challenges to demonstrate skills for bragging rights or increasingly large prizes.

Portia Pusey provides educational research and research development services for projects that improve our national preparedness to protect our digital infrastructure by enriching the engagement and professional skills of cybersecurity learners and professionals. Her research interests center on cybersecurity competitions as a sport and the potential of competitions to function as professional development, learning environments, and assessment. She specializes in leading the design, conducting, and performing analysis of research that strengthens practice in formal and informal cybersecurity learning situations. She also designs outreach experiences that promote cybersecurity careers and awareness for all k-career stakeholders. She is fluent in academic and technical jargon and often serves as a bridge when working with interdisciplinary academic and professional teams in technical fields. edrportia@gmail.com

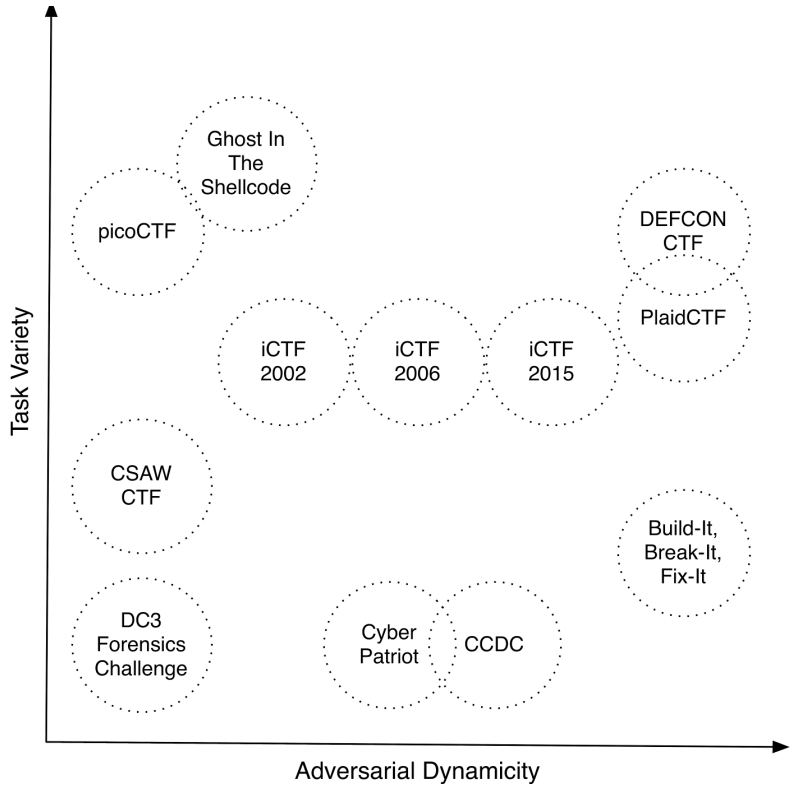

Figure 1: A common but somewhat misleading characterization of cybersecurity games, which ignores a game's intended audience, re-playability, and usefulness in an education setting—all identified as meaningful qualities by the security game community.

Taxonomies for Cybersecurity Games

No game on its own can possibly satisfy all the demands of every player. Imprecision in communicating requirements, outcomes, and mechanics means some players may not be able to identify games appropriate to their goals. To avoid player disappointment, competition Web sites sometimes identify both what they are and what they are not, clarifying where established language is imprecise and terminology is confusing. The "capture the flag" term has become especially problematic within the community; it is a powerful descriptor for a wide audience but too broad for players seeking a specific type of game or experience.

The two factors of cybersecurity games most frequently discussed, either explicitly or implicitly via comparison, are (1) whether the player will be either attacking or defending a network, service, or digital asset, and (2) whether the player will be attacking other players. While these factors are more easily characterized at their extremes, they can be imagined as a continuum, encompassing the dimensions of task variety and adversary dynamicity (see Figure 1). Task variety considers the types of knowledge, skills, and abilities players need to demonstrate during the competition. At one end of task variety are games that mix attack-defend mechanics with a variety of domain-specific challenges, typically requiring a team due to complexity and scope; at the other end are games that focus on a narrower variety of skills, like service hardening or reverse-engineering challenges. At one end of adversary dynamicity are games featuring pre-created challenges, where the game adversary's strategy is "baked" into the competition by the designer; at the other end are games where opposing players control the game adversary's strategy, allowing it to be arbitrarily complex and highly dynamic.

Characterizing games along these two dimensions, however, may be overly simplistic, artificially constraining, and misrepresent the quality of the event. Indeed, we believe all the games identified in Figure 1 are fun, effective, and enjoyable to a variety of audiences. What's more, our community discussion at 3GSE '15 highlighted that players care about many game attributes beyond these dimensions. Novice players want exercises that progressively build technical skills and self-efficacy in an environment that is unintimidating. Instructors seeking games to complement the curriculum want challenges that highlight specific learning objectives and persist after the competition ends, allowing continued use in the classroom. Designers want to develop entirely new genres that share and play with traditional CTF ideas, without fear of mischaracterizing themselves. Normative, secondary terminology could acknowledge and highlight these features, when present.

One problem with characterizations of task variety is that they tend to perpetuate a false dichotomy between attack and defense. Some games designers feel obligated to limit themselves to defense-only skills or sysadmin skill building. This may encourage some players to participate, communicating that game skills are relevant to an accessible, well-defined profession, such as "network security administrator," compared to the less understandable profession of "security consultant." This may also be to avoid any impression of "hacker training" or otherwise serving as a training ground for unethical skills. Limiting tasks in this way, however, likely underestimates the value and mischaracterizes the intent of offensive skills. As with all types of games, offensive and defensive skills are very related—some experts claim learning to attack is prerequisite to effectively defending. Learning to analyze and patch a vulnerable binary is, perhaps, an improperly structured version of the exercise in which one analyzes a binary, demonstrates how to exploit it, and then patches it. Further, characterizing games along this continuum may underemphasize essential technical and social skills exercised during the game, such as writing code in a team (e.g., Build-it, Break-it, Fix-it [3]) or reasoning about game-theoretic cost-benefit tradeoffs (e.g., 2011 iCTF's point-laundering scoring mechanism [4]).

The problem with characterizations of adversary dynamicity is that they tend to perpetuate the myth that human opponents are more dynamic, less predictable, and more skilled than the non-player adversaries encoded in challenges. Automated systems can be dynamic and arbitrarily complex. The term "adaptation" is employed for games where the obstacle is changed to challenge the player at an appropriate level, creating an experience of flow. In contrast, player adversaries could be considered "poorly designed": they can become distracted, become disengaged, be offline for significant portions of the competition, be over-skilled (or under-skilled) compared to other players, etc. The systems performing in DARPA's Cyber Grand Challenge are demonstrations, in some ways, comparable to IBM's Watson competing on *Jeopardy*. Their performance may hint, among other things, at the potential for non-player adversaries in cybersecurity games. Perhaps, in the future, some of the most dynamic, educational, fun and challenging experiences may be *Jeopardy*-style "beat the expert system" competitions.

One factor of frequent discussion for cybersecurity games is their potential relationship to education and training. Organizers are certainly designing in such opportunities, despite the lack of appropriate terminology. The NSA's Codebreaker challenge is one such example. It is a multi-month, online, *Jeopardy*-style, reverse-engineering competition where challenges are parametrized for each player. Correct solutions yield links confirming completion, making it possible for instructors to assign the challenges as extra credit and get proof of student achievement.

One might try to develop a taxonomy characterizing the role of a cybersecurity game in instruction or its placement within formal educational curricula; however, to date, games have yet to evolve into full, online courseware. Instead, it may be more appropriate to consider cybersecurity games as "informal learning spaces," like museums, libraries, and makerspaces [5]. They can be practice spaces for hands-on activities—opening up opportunities for tinkering, improvisation, failure, and sharing—in an authentic yet safe environment. They can be enriching virtual environments with embedded opportunities that teachers may leverage, while avoiding the suggestion that games supplement instruction or shoulder specific classroom goals. Just as teachers need to develop strategies to adjust instruction to get the most out of a field trip, the same may be true for cybersecurity games. Those game designers seeking to curate such an environment may benefit from lessons learned by other informal learning spaces. For example, the idea of participatory experiences and co-creative design may help designers evolve the game in response to individual and community goals [6].

While a community discussion about terminology may appear pedantic to some, it has highlighted some essential questions and core values about game objectives (which is, perhaps, a separate and similarly controversial subject). The discussion demonstrates the struggles our community faces when presenting new games to established players, designing games to reach new players, and interfacing with educators for use in clubs and classrooms. It further suggests missing research on who players are and what they need from the cybersecurity community. Ultimately, discourse that includes building a common body of terminology also will help us to be more aware of our values and goals.

ASE and the Future of 3GSE

In response to the USENIX community's interest in security education research, more broadly, the 3GSE workshop has been expanded and rebranded as the USENIX Workshop on Advances in Security Education (ASE), a new USENIX workshop designed to welcome a wider range of contributions to security education research. ASE '16 will be co-located with the 25th USENIX Security Symposium, to be held in Austin, TX in August. We hope to see you there!

Acknowledgments

The authors would like to thank the National Science Foundation for their generous contributions to 3GSE, through awards #1140561 and #1419318.

References

[1] CTFtime: ctftime.org.

[2]Andrew Ruef, Michael Hicks, James Parker, Dave Levin, Atif Memon, Jandelyn Plane, and Piotr Mardziel, "Build It Break It: Measuring and Comparing Development Security," *Proceedings of the USENIX Workshop on Cyber Security Experimentation and Test (CSET),* 2015: https://www.usenix.org/conference/cset15/workshop-program/presentation/ruef.

[3] Masooda Bashir, Jian Ming Colin Wee, April Lambert, and Boyi Guo, "An Examination of the Vocational and Psychological Characteristics of Cybersecurity Competition Participants," *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE),* 2015: https://www.usenix.org/conference/3gse15/summit-program/presentation/bashir.

[4] Yan Shoshitaishvili, Luca Invernizzi, Adam Doupe, and Giovanni Vigna, "Do You Feel Lucky? A Large-Scale Analysis of Risk-Rewards Trade-Offs in Cyber Security," *Proceedings of the 29th Annual ACM Symposium on Applied Computing,* 2014.

[5] Andrew Richard Schrock, "'Education in Disguise': Culture of a Hacker and Maker Space," *InterActions: UCLA Journal of Education and Information Studies,* vol. 10, no. 1, 2014.

[6] Nina Simon, *The Participatory Museum,* Museum 2.0, 2010.