The Importance of Using Hacker Contests and Mindset in Teaching Networks and Information Assurance

Thomas A. Babbitt

This paper was completed and submitted in partial fulfillment of the Master Teacher Program, a 2-year faculty professional development program conducted by the Center for Teaching Excellence, United States Military Academy, West Point, NY, 2011.

There is a small but growing body of literature focused on the way in which hackers approach a problem and learn how computer systems work both independently and more importantly networked. This literature includes the manner in which hackers teach themselves through forums and self study and the way in which they test their acumen in competitions designed to increase both their knowledge and skill set [1,2,3]. The word hacker can imply a negative connotation; this paper uses the purest definition of a hacker as an, “individual who creatively explores technology and pushes it in innovative directions [3].”

Educators can learn from the contests that are run at hacker conventions. Adaptation of these contests is pedagogically sound and can lead to significant student learning in computer and social networking as well as information security. Attending, presenting at, and better yet inspiring students to attend and present at hacker conferences can significantly increase the value of, and reinforce objectives taught in class [4]. Understanding how applications are written and the potential security issues is paramount to writing good code. This has lead to modifications in how some instructors teach programming [5].

Design of courses in Computer Science (CS), Information Technology (IT), and Information Assurance (IA) can and should take into account how hackers learn and modify some of the contests that are run at hacker conventions for use in the classroom [6,7]. In fact, programs as a whole in CS and IT can be modified. The Accreditation Board for Engineering and Technology (ABET) publishes accreditation requirements each year. Included in those requirements are a number of student outcomes that each program must meet [8] in order to attain accreditation. Many of those outcomes can be met or augmented by contests modified from hacker conventions. While the merit, requirement, or necessity for ABET or any other accreditation is outside of the scope of this paper; the idea that the hacker mindset and modification of hacker contests as part of CS, IT, or IA education is not mutually exclusive from, and in fact falls within, the student outcomes required for accreditation.

Included are some major topics in CS, IT, and IA education where hackers have created and competed at hacker conventions that have been and can be modified for further use in the classroom.
Network Warfare: One of the first and longest enduring competitions is capture the flag (CTF). These competitions challenge teams to attack and defend computing resources. These exercises are run by security experts such as DDTek, Kenshoto, and the Ghetto Hackers. There have been numerous academic adaptations to include the Collegiate Cyber Defense Competition (CCDC) [9] and the National Security Agency sponsored Cyber Defense Exercise (CDX) [10].

Wireless: Most students employ at least one, if not multiple devices that have wireless capability. Hacker competitions have led to a better awareness of wireless security issues. To explore and show the vulnerability of wireless in conjunction with social engineering, the HOPE conference issues electronic badges to volunteers, that tracked location and demographic data. This dataset is currently available for research at Dartmouth’s CRAWDAD wireless research repository [11]. The hacker mindset for learning networking and its contrast with how networking is currently taught to undergraduates is highlighted in a number of works.

Cryptanalysis: "Hacker conferences use cryptographic competitions to great effect. The badges at Shmoocon and Toorcon have included subtle codes, puzzles, and clues. Other conferences have disseminated code breaking contest sheets to attendees and awarded prizes at the conference’s closing ceremonies. Importantly, some competitions require winners to share their techniques for the benefit of all. DEFCON’s recent Crack Me if You Can hash cracking competition challenged participants to illustrate weaknesses in the username/password paradigm by working backwards from hashes to passwords. [3]"

Social Engineering: This is the art of using social situations to gain access to restricted areas or data. This can be as simple as pretending to be the IT department either on the phone or by e-mail and asking someone for their log in credentials stating that they need to be updated immediately. There are many hacker competitions such as Social Engineering CTF competition at DEFCON where teams try and social engineer a target company and then have 20 minutes to attach during the competition.

Hardware Hacking: There are contests at hacker competitions where the goal is to modify a hardware device to do something that it was not intended to do. Each year at DEFCON the badges are a hardware device and there is a competition to see who can modify the badge to do something unintended.

Security Coding and Malicious software: There are many hackers that attempt to attack application software such as the browsers, mail clients, word processors and document viewers. There are a number of hacker competitions where contestants modify code to attempt to bypass anti-virus software, while still maintaining a functional payload. There
are also academic professionals who require attack scripts to be created and turned in with each homework assignment to help teach the importance of good coding [5].

Physical Security: This is one of the most overlooked aspects of Information security. Most hacker conferences have lock picking competitions, workshops, and labs to provide lock picking techniques. An "example is Toorcon’s Tamper Evident contest, which challenged participants to bypass purportedly tamper-resistant technologies, thus testing vendor security claims [3]."

The categories of competitions above are not exhaustive. The point is that there are a wide variety of different competitions that occur at hacker conventions, many of which can be modified for use in the classrooms. Doing so introduces the possibility to create a very rich learning environment, but for this environment to flourish there must be an incentive to compete. At hacker contests, there are award ceremonies and in many instances prizes for the winner. In one such competition, if you hack into the computer you own it. Similar incentives must occur in the classroom. Student effort and success in the competition must in some way reflect on their standing in the class.

Due to the nature of many of the skills taught and required for successful participation and victory in hacker competitions, there might be some hesitancy to teach these skills. The benefits far exceed the risks, but there must be a solid ethical component to all courses that utilize the hacker mentality or modify contests for use in class. Instructors must, from the beginning, set the correct tone and teach the proper use for the skills learned. They must articulate the pitfalls and have in place standards. If students use their knowledge maliciously, instructors must discuss with and reprimand students.

Conclusions and Recommendations: There are a couple of key points necessary when using competitions modified from hacker conventions. The first is that the competitions must be engaging and that there must be some significance in terms of perforce that is associated with the competition. It must count towards part of a student’s grade. The second is that the correct ethical tone must be adopted from the beginning. Students must understand that some parts of a game or competition set in a controlled environment in class are acceptable, but those same actions or techniques used on their friends, businesses or the government can be illegal. Finally, enjoy bringing new and challenging competitions to the classroom. Student will enjoy them and learn significant skill sets. All of these concepts should be routed in some student outcome, whether outlined by ABET or through the design of the course. Instructors should attend a hacker convention and listen to the speakers, watch the competition, interact with other attendees, and present academic work in Information Assurance.
Annotated References


The author discusses the differences in the ways that hacker and traditionally trained programmers attack a problem and suggests that there is much that can be learned from how hackers learn. The author discusses the lack of understanding of the lower layers of an operating system and how application interfaces are written. This can lead to security holes created when developing software. The author discusses the lack of academic literature written about the underlying systems and in how hackers learn. To create his course in programming security he reverted to taking well written articles from hacker websites.


The author discusses how a hacker learns about networking and networking security. He proposes that there are three parts to that education. The first is understanding and monitoring network messages and formats at each level down to and including the bits. The second is to inject arbitrary data into correctly formed packets to test boundary conditions. The third is to determine implementation peculiarities and attempt to exploit them.


This paper discusses the untapped potential of hacker competitions. It goes through a number of types of competitions and the success in the past of modifying competition for academic use. It suggests that there is still a large untapped series of hacker competitions that can be modified for classroom use.


The author suggests that academic professionals can learn from the hacker community. While many that attend might not appear the same or have the same degrees as those in academia, they are very competent in their field and are more than willing to discuss very technical topics. If given a chance they can and will give constructive feedback on research topics.

The authors in this paper propose the use of attack scripts as a method of teaching security concerns when coding. He forces his students to turn in an attack script capable of attacking some part of each coding assignment. The author understands the difficulty of teaching the basics to include checking function or method returns, memory management, and expectation handling. He suggests giving students a framework for creating attack scripts against their homework assignments as a way to teach the necessity to take security into account when coding.


The authors in this work discuss the multiple course sequence in Information System Security that they overhauled. They work through the pedagogical rational for their choices in courses and topics. The precipitous for the change was due to the lack of hands on understanding of how networks and computers were vulnerable. They validated there result with a first place win against seven other educational institutions in the 2006 Midwest Regional Collegiate Cyber Defense Competition.


This paper explores the use of simulation games to teach Information Assurance. The paper discusses an author created game created called CyberCIEGE. The game is similar to the series of games created by SIM. The instructor can create a scenario and the students then play the game. Their decisions on risk can lead to network compromise. Winning is determined by mitigating risk and selecting the proper equipment and services to use.


This lays out the student outcomes for CS, IT, and information systems ABET accreditation. It discusses what is required to be ABET accredited. Below is a list of the student outcomes.

All Majors (CS, IT, and Information Systems)
(a) An ability to apply knowledge of computing and mathematics appropriate to the discipline
(b) An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution
(c) An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs
(d) An ability to function effectively on teams to accomplish a common goal
(e) An understanding of professional, ethical, legal, security and social issues and responsibilities
(f) An ability to communicate effectively with a range of audiences
(g) An ability to analyze the local and global impact of computing on individuals, organizations, and society
(h) Recognition of the need for and an ability to engage in continuing professional development
(i) An ability to use current techniques, skills, and tools necessary for computing practice.

Computer Science

(j) An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices. [CS]
(k) An ability to apply design and development principles in the construction of software systems of varying complexity. [CS]

Information Systems

(j) An understanding of processes that support the delivery and management of information systems within a specific application environment. [IS]

Information Technology

(j) An ability to use and apply current technical concepts and practices in the core information technologies. [IT]
(k) An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems. [IT]
(l) An ability to effectively integrate IT-based solutions into the user environment. [IT]
(m) An understanding of best practices and standards and their application. [IT]

This paper discusses the significance of the first Cyber Defense Competition and how it came into existence. It highlights why the competition came into existence and the necessity of the skill sets required to compete. It showed some significant shortcoming of information security education.


The authors discuss the importance of the CDX to different participating service academies. This paper talks about some of the changes over time and the relevance to the future leaders of the country to understand the threat and to envision how to create systems that mitigate some of the risk.

References