Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

Providing an Undergraduate Research Experience in a Senior Level Security Course

Dino Schweitzer, Jeff Boleng, and Steven Hadfield, *United States Air Force Academy*

Abstract – ***Student research can be a powerful educational tool whose benefits are touted by educators at both the graduate and undergraduate levels. Providing a meaningful research experience at the undergraduate level faces several challenges as students are less academically mature, have limited time, and do not have an extensive knowledge base to draw from. Creation of a successful research experience as part of a course project requires careful planning in terms of available topics, project structure, and faculty oversight. At the Air Force Academy, we teach a hands-on senior level security course with a final project. We have structured the final project to attempt to provide a realistic research experience for our students. This paper will describe some of the challenges and approaches to undergraduate research, detail the approach we have taken in our security course, and share the results of our experience.***

Index terms – Computer Security, Security Education, Undergraduate Research

I. BACKGROUND

Research at the undergraduate level has long been recognized as a valuable tool for stimulating intellectual growth, motivating development of learning skills, and achieving higher levels of cognitive thought [1]. Studies have shown that undergraduate research experiences can aid in both retention and advancement to graduate studies [2]. Within the context of a rapidly evolving and highly dynamic field such as computer security, research skills are quite simply essential for survival and success. Therefore, we see the development of research skills as an inherent and required component of computer security education. In this background section, we will briefly review the challenges and approaches to research in undergraduate education; look at the different approaches to computer security education and the role of research in these approaches; and overview how both computer security and undergraduate research are addressed at our institution.

The above stated advantages of an undergraduate research experience come with challenges. Providing an undergraduate research experience is labor-intensive for the faculty, demanding of faculty expertise, and needs time for students to develop the necessary skills as well as to practice and mature in the disciplines of research [3]. To reap the benefits of an undergraduate research experience while navigating the challenges, a variety of approaches have been pursued. A typical approach makes use of opportunities outside of a recognized course such as independent research projects with a faculty member or summer research programs. Another approach is to integrate a research experience into a senior capstone project course [4]. Some efforts have even targeted freshman courses [1]. In order to overcome some of the challenges with moving students into productive and effective research, some universities and colleges have introduced research methods courses into their undergraduate computer science curriculum [5].

As a dynamic field of study with many emergent technologies, computer security provides fertile grounds for the integration of an undergraduate research experience [3]. Furthermore, one could easily argue that the development of complex, critical, and creative inquiry skills fostered by a research experience are requisite for such a rapidly evolving discipline. Approaches to computer security education naturally dovetail with aspects of a successful research experience. Active and experiential pedagogies are inherent in a research experience and have proven most beneficial to computer security education [6]. Ethics and professional responsibility are critical to both research and computer security education as well [7]. Just like a biology or chemistry research lab need appropriate safety measures, computer security education requires segregated 'sandbox' networks where effects of potentially harmful tools and techniques can be explored without adverse effects [8].

At the United States Air Force Academy, computer security takes on a role of primary importance. All computer science majors must take at least one course related to computer security. To fulfill this requirement, we have a suite of computer security courses which include our cornerstone course in computer security and information warfare, a separate course in computer network defense, and a course in cryptography. Computer science students completing all three of these courses earn a special designation on their transcripts showing their major as "Computer Science – Cyber Warfare". The cyber warfare track is very popular

Academy Center for Cyberspace Research
Department of Computer Science
United States Air Force Academy, CO 80840
dino.schweitzer@usafa.edu

drawing over three-quarters of our computer science majors.

Historically, our cornerstone security course in computer security and information warfare has taken a very hands-on, experiential approach balancing conceptual and practical topics within security education. Included within this course design are in-class labs using various tools for exploring computer security topics and participation in student 'capture the flag' competitions with other colleges and universities in the state [9]. Additionally, the course consistently included a significant course project which involved topics such as security tool development or focused exploration of some course topic. We have recently re-vectored the course project to much more of a research activity as part of a deliberate and intentional effort to provide a developmental research experience throughout our computer science program.

In the last few years, we have evolved a department initiative to integrate a developmental research experience across our computer science curriculum. In our first-year introduction to computing course required for all students, we develop information literary skills by having students research seemingly outlandish claims using the Internet. With this activity, the students develop and practice Internet search skills as well as the ability to assess and cross-check the legitimacy of information. Computer science majors in their sophomore year develop teamwork skills via group programming projects in both their CS1 and CS2 programming courses. Also during that year, they develop skills designing experiments with a memory cache simulator exercise in their computer architecture course [10].

In their junior year, computer science majors further develop research-related skills with two exercises in their programming paradigms course. The first such exercise presents the student with a vaguely defined topic area, such as artificial life flocking behavior, and asks the students to first research the topic and write up a technical research paper describing the topic. This helps to develop their literature review and technical writing skills. Then they are tasked to implement a simulation demonstrating the phenomena [11]. Also, in the programming paradigms course, the computer science students individually research and present an oral report on a programming language not addressed elsewhere in our curriculum. Between their junior and senior years about a third of our computer science majors are given the opportunity for a five-week summer research experience typically with an Air Force laboratory or Department of Defense research agency. At the conclusion of these experiences, the students develop a research report and deliver a presentation to the faculty and their fellow cadets.

Our deliberate undergraduate research experience approach culminates during the students' senior year. In their two-course software engineering capstone sequence, they work in teams of five on a software development project for a real customer. Care is taken with selection of project topics so that each team must learn some new language or technology to which they have not yet been exposed. Topics are purposefully ill-defined and frequently involve some type of data collection and analysis to demonstrate the impact of what they have developed. The teams must also present their work at some appropriate, external professional research forum. In addition, the students have opportunities to conduct individual research with faculty members on topics of their choice for academic credit and must write up and present the results of those efforts.

Finally, these senior computer science students use the research skills developed throughout our curriculum to conduct a two-person team research effort as a primary component of their computer security and information warfare course. This research assignment is the primary focus of this paper.

II. APPROACH

We approach the student research project in our senior level security course in a similar fashion that a graduate advisor guides their students. The key differences are the compressed time scale and student preparation level. We address these two differences through careful project selection, multiple project submissions, and active project mentoring.

A. Project selection

Students work in teams of two and are allowed to select any research area or topic they choose. Each team has a faculty member serving in the role of "project mentor" for the research. Working in two-person research teams with a mentor provides the ability to experience team dynamics and affords the ability to share the load, while still avoiding the potential for some team members to "hide" or not pull their full weight. In order to help students get started, a list of available project mentors and associated research areas are provided at the start of the semester. The research areas are general security topics that mentors identified as having existing projects, ideas for projects, or sufficient experience to identify a project and mentor a team. The initial list of areas is shown below:

- Vulnerability Software Assessment
- Honeypots
- Botnets
- Steganography
- Digital Camera Forensics

- Graphical Passwords
- Smart Card Vulnerabilities
- Security Visualization
- RFID Technology
- Flash Memory Vulnerability
- Wireless Denial of Service
- Computer Security Situational Awareness

Based on this list, the students select an area of interest and meet with the associated mentors to iteratively define their specific project and refine their research goals. No attempt is made to establish a firm research plan up front. Rather, the mentor guides the team through the current state of the art in the area by helping identify sources and directions for them to perform an abbreviated literature review. Care must be taken to keep the students focused on the most important information sources and background articles available in the research area. Since students do not have much experience with conducting literature reviews for research, guidelines are provided which points them to specific resources and approaches.

As the student teams explore the research area, they may conceive of a novel approach or solution to outstanding problems, but it is often outside the scope of a one-semester project. The faculty mentor must guide them deliberately to a more realistic project statement and goal. Ideally, projects and goals are defined that are 1) achievable given their background, skills, and education level, 2) practical within the timeline of a semester project, and 3) meaningful and relevant enough to demonstrate the full research experience. As an example of the types of research conducted, the final list of selected projects for the Spring 2009 semester is shown below:

- Detecting keyboard pattern passwords
- Vulnerability assessment of Fourier-Mellin watermarks
- Vulnerability assessment of Multipurpose Watermarking method
- Locating rogue access points
- Botnet capture and analysis
- Detecting digital image tampering
- Developing parallel algorithm for jam resistance encoding
- Measuring effectiveness of risk assessment software
- Visualizing cyber situational awareness architecture
- Develop a command and control for P2P botnets
- Parallel processing to speed up WPA cracking
- Analysis of steganography in GIF animations

B. Multiple project submissions

Achieving a meaningful research experience in a single semester requires dedicated progress in a timely manner. In an effort to ensure the student teams stay on track, the project is broken into a series of five intermediate turn-ins. These submissions serve to guide the teams along a well-defined research approach and avoid last minute surges of effort that can be typical of heavily loaded undergraduates. Our required submissions, their associated timing, and relative weight are:

1. *Team members and topic selection, due 12.5% of the way into the semester worth 0%*
   This submission consists of team member names (2) and a research area. Previous instructor approval is required if the research area is not on the topics list. Multiple teams may select a similar topic, but the specific research project to be accomplished must be distinguishable. Before submitting the topic, teams meet with the associated faculty mentor to fully understand the nature of the topic and possible research projects.
2. *Background report, due 25% of the way into the semester worth 10%*
   This is a 4-6 page, double-spaced research paper that provides background on the selected topic, why it is important to computer security, and a summary of current techniques for solving the problem or dealing with the issue. The report should include at least five technical references (not URL's). The report is graded on technical writing skills, technical content, and quality of background research. Teams work closely with their faculty mentor to ensure an adequate understanding of the problem and existing solutions for dealing with it. At this point, students are purposely told to not address their specific proposed approach, but to focus on the area in general to understand the problem in greater detail. To assist students in proper format and content, a report template and sample paper are provided.
3. *Research design and plan, due 35% of the way into the semester worth 10%*
   This is the proposal of what students will accomplish in their project. Based on their background work, they identify a specific goal for the project that they are trying to achieve. This should be something unique that is not just a re-implementation of previous results. The document includes the specifics of how they are going to accomplish their goal and assess the results. Total length for this section is 2-4 pages. This section is the crux of what their project is, and requires careful coordination with their

mentor to ensure it is unique, accomplishable, and follows a well-defined research approach.

4. *Implementation / experiment, due the next to last lesson of the semester worth 30%*
   The nature of the implementation / experiment depends on the selected project and proposed approach. If software is developed, it must be well-documented. A written description must accompany any implementation explaining its use and any necessary operating instructions. The implementation is graded based on how well it performs, how closely it matches the proposed plan, and the quality of the accompanying description. In the case of experimental results, the steps and details of the data collection, steps followed, and analysis must be thoroughly explained.
5. *Final report and poster, due the final lesson of the semester worth 50%*
   The documentation of their research includes both a final report and a technical poster for presentation. The final report consists of the overall results of the project. The goal is to write it as if it were a paper submitted to a technical conference for publication. It contains the background report previously submitted, the same content as contained in the poster in written form, and any associated user guides or documentation for the implementation. The final report grade is based on writing style, completeness, quality of analysis, results, and conclusions. The purpose of the poster is to allow students to display their results in a professional format for presentation at a technical forum. Students are provided with PowerPoint poster templates that they can use to organize their results. Students can submit their PowerPoint files to the department for printing on a large-format printer. This ensures quality of the final result and teaches them about proper poster formatting. The posters are placed on display and reviewed by Computer Science faculty during class time on the final lesson of the semester. Students must be available by their poster to answer faculty questions. Faculty evaluate the posters and the student's ability to successfully answer questions about it as part of their final grade.

The above graduated submission requirements, combined with active project mentoring, allow students to stay on track and have the framework for a complete and significant research experience.

C. Active project mentoring

Active and engaged project mentors are essential to the success of our undergraduate research projects. It is important that the mentors have research experience themselves as well as a deep knowledge of the area of research the student team will be investigating. We require at least weekly meetings between research teams and their faculty mentors to review status and plan subsequent actions. Meeting more often for brainstorming and guidance is highly encouraged.

In addition to providing background expertise, faculty mentors assist with accountability and introduce the students to a healthy, well-structured mentoring relationship. Faculty mentors review all materials and research before they are submitted for grade. These reviews act as direct feedback to the students as well as help ensure consistent quality and effort for each submission. The reviews also require the teams to work well in advance of a deadline and encourage them to start early and work often - admirable work habits to develop in their own right.

III. OUR EXPERIENCE

Spring semester 2009 is the first semester we have fully implemented this approach in the security course project. To attempt to measure the impact of providing a research experience, we initially gave the students a pre-survey on their attitudes toward research and their ability to perform it. Students were asked to self-rate themselves on a scale of 1-5 (1 being lowest) in 14 research-related areas. The areas and results are shown in Table 1.

Average Rating	Area
3.3	Understanding of research process
3.3	Understanding how computer scientists think
3.2	Understanding how to investigate literature
4.0	How to work effectively with others
4.5	How to work independently
4.1	Tolerance for obstacles
4.5	Importance of ethical conduct
3.8	Ability to analyze data
3.9	Skill in interpretation of results
3.9	Skill in oral presentation
3.3	Skill in scientific / technical writing
3.5	Self-confidence in conducting research
3.5	Desire to conduct additional research
4.0	Desire to attend graduate school

Table 1. Research attitudes pre-survey results.

Not surprisingly at our institution, students exhibit high self-confidence in their ability to work both independently as well as in a team environment. They believe they have a tolerance for obstacles and strongly understand the importance of ethical conduct. They are less confident in their understanding of how to conduct research, perform

literature searches, and write technical documents. The technical writing came as somewhat of a surprise as our students have multiple opportunities to write in both their computer science and other coursework. However, the early turn-ins of their project reports demonstrated that their self-assessment was correct and there was room for improvement regarding technical writing skills. As a direct result of this weakness, additional resource materials and guidance for mentors were provided to assist the students in documenting their results. Also, in reaction to the survey results, additional guidelines for how to conduct a literature review were provided.

At the end of the semester, a post-survey will be conducted to see if attitudes have changed as a result of going through the research experience. Additional questions will include a rating of the overall experience, the value of faculty mentors, and suggestions for improvement. Results from this survey and our experience with this approach will be posted to our web site at www.usafa.edu/accr.

Several observations can be made about the effectiveness of this approach to date. One of the key observations is the critical role that the faculty mentor serves. The level of assistance, direction, and "mentorship" provided by the mentor makes a huge difference in the student attitude about their project and the quality of their work. Several individual and group meetings have been held with mentors to discuss their role, to provide guidance on how to direct their teams, and to encourage frequent interaction with their students. Senior researchers are not always the best mentors. Nor are junior faculty members who may have a close working relationship with students, but have not had a lot of experience in conducting research of their own. The best mentor relationship is one in which the mentor becomes actively involved with the students project offering guidance, ideas to consider, and positive motivation. For future offerings of this course, much more guidance will be provided to mentors up front describing their role, expectations, and the time commitment required to be a successful mentor.

Another observation is that the list of topic areas provided was a good start in narrowing down the field of possible topics, but the list needed to be even narrower. One of the largest challenges in conducting a semester-long project is the need to quickly define exactly what the project is going to be so students can conduct an adequate background investigation in a timely enough fashion to actually define and conduct unique research with their topic. While the list of general areas was better than leaving it totally wide open, which was the case in previous semesters, it was still too broad. For example, asking students to survey the field of "botnets" to define a specific research topic was extremely difficult as there are so many different aspects and possibilities. For future years, topics will be broken into both the general area, such as "botnets", as well as subtopics that can more quickly focus students' background work. For "botnets" such subtopics could include detection, command and control structures, as well as botnet capture and analysis. In practice, this happened with mentor interaction. Explicitly stating the more detailed topics up front and having mentors have some specific possible projects in mind will facilitate students getting to the meat of the project more quickly.

One of the common questions asked by teams was whether an idea to pursue was really research, or simply a replica or re-implementation of someone else's work. At the graduate level, students would have more time to do a sufficiently thorough background investigation to answer this question directly. For purposes of this project, the mentor was relied upon to provide that insight. All projects were required to have some unique aspect that had not been documented in the literature.

A final observation as to our experience to date is that while students are often good at coming up with ideas of things to try, they are extremely inexperienced in judging the difficulty of implementing something, in analyzing the results of their work, and in understanding the relationship of their efforts to other research that has been accomplished in the area. The students' ability to come up with novel and radical ideas may be a result of not already being familiar with conventional ways of thinking about a particular type of problem. On the flip side, that same lack of knowledge can bring a fresh look to the problem and suggest approaches that may have merit. However, their lack of experience often results in a large underestimation of the amount of time it will take to implement something, to capture data, to conduct experiments, or to complete a research step. The typical undergraduate approach of waiting until the last minute to complete a project does not work in a research project. The role of mentor is critical here to constantly monitor the team's progress, help provide realistic estimates of time and effort, and keep them on track. Similarly, even once the team has achieved some results, they do not know how to evaluate these results. Whether it is a statistical analysis, comparing different approaches, or recognizing the implications and limitations of their approach, they tend to be very narrowly focused on their solution. Once again, the role of the mentor is key to helping them see the larger picture and how to conduct meaningful analysis.

IV. CONCLUSION

Research can be an effective way to teach undergraduate students about a rapidly changing and complex field such as computer security. They gain detailed knowledge about a focused area within the field, they learn

techniques for how to conduct investigations, and they (hopefully) gain confidence and motivation for advanced study and research. To be successful, students need to view the experience as a positive one, both in terms of being enjoyable and ideally producing something worthwhile. Our hope is to have several of the student projects published in a suitable venue. Getting a publication will help with the students' perception of research being a meaningful exercise and motivate further exploration.

To address the limitations inherent to undergraduates, it is necessary to carefully structure the project with phased turn-ins, to provide templates and examples, to help narrow their selection of a project up front, and to provide encouragement and assistance throughout. The greatest factor in making it a productive and positive experience is the faculty mentor. A well-prepared and active mentor can provide outstanding direction, be highly motivating, and serve as a role model for conducting successful research.

We will continue to use this approach for the final project in our senior level security course. We will make some minor adjustments based on our experience and student feedback. We will also begin working even earlier in the process identifying mentors and projects, providing guidance to mentors on how to be effective, and motivating future students with the opportunities afforded by this approach.

V. References

[1] Becker, K. (2005). Cutting-edge research by undergraduates on a shoestring? Journal of Computing Sciences in Colleges 21, 1.

[2] Dahlberg, T., Barnes, T., Rorrer, A., Powell, E., Cairco, L. (2008). Improving Retention and Graduate Recruitment through Immersive Research Experiences for Undergraduates, Association for Computing Machinery Special Interest Group in Computer Science Education (SIGCSE 2008).

[3] Knox, D. L., DePasquale, P. J., Pulimood, S. M., (2006). A Model for Summer Undergraduate Research Experiences in Emerging Technologies. Association for Computing Machinery Special Interest Group in Computer Science Education (SIGCSE 2006).

[4] Hadfield, S., Jensen, N. (2007). Crafting a Capstone Software Engineering Project Course. Journal of Computing Sciences in Colleges, 23, 1.

[5] Polack-Wahl, J. A., Arewalt, K. (2006). Learning Strategies and Undergraduate Research. Association for Computing Machinery Special Interest Group in Computer Science Education (SIGCSE 2006).

[6] Schweitzer, D. and Collins, M. (2006). Teaching computer security concepts - let's get physical! Proceedings of the Annual Conference on Education in Information Security, (ACEIS'06).

[7] Peckham, J., Stephenson, P., Herve, J-Y., Hutt, R., Encarnacao, M. (2007). Increasing Student Retention in Computer Science through Research Programs for Undergraduates. Association for Computing Machinery Special Interest Group in Computer Science Education (SIGCSE 2007).

[8] Conklin, A. (2005). The Use of a Collegiate Cyber Defense Competition in Information Security Education. Proceedings of the 2nd Annual Conference on Information Security Curriculum Development (InfoSecCD '05).

[9] Schweitzer, D., Gibson, D., Collins, M. (2009). Active Learning in the Security Classroom. Proceedings of the Hawaii International Conference on System Science (HICSS-42).

[10] Coutinho, L., Mendes, J., Martins, C. (2006) MSCSim – Multilevel and Split Cache Simulator. Proceedings of the 36th Annual Frontiers in Education Conference.

[11] Hadfield, S., Weingart, T. (2008). Interdisciplinary Research, Writing, and the Computer Science Programming Exercise. Association for Computing Machinery Special Interest Group in Computer Science Education (SIGCSE 2008).