An Experience Report on Undergraduate Cyber-Security Education and Outreach

Michael E. Locasto
George Mason University
mlocasto@gmu.edu

Sara Sinclair
Dartmouth College
sinclair@cs.dartmouth.edu

ABSTRACT

We report on the design and execution of an ambitious, innovative, and comprehensive program of education, training, and outreach in information security. This program, SISMAT (Secure Information Systems Mentoring and Training), aims to foster expertise in computer security at the undergraduate level.

SISMAT consists of three major components. First, an intensive two-week seminar and laboratory course provides participants with a foundation in computer security. Second, SISMAT personnel coordinate with participants and industry, non-profit, and government organizations to help place participants in internships related to information security and assurance. Third, SISMAT personnel coordinate with participants' faculty mentors to identify and develop a suitable mentored research project for the SISMAT participant in the semester following the internship. In this way, SISMAT helps foster the growth of security curriculum derived from the advice and guidance of recognized industry and academic experts in information and computer security.

Categories and Subject Descriptors

K.7.1 [**The Computing Profession**]: Occupations

General Terms

Security

Keywords

cyber security training, SISMAT

1. INTRODUCTION

Organizations face a critical scarcity of well–trained expertise in information security. Many of our colleagues in industry, government, and non-profit institutions have expressed difficulty finding personnel with appropriate training in cyber security tools. At the same time, information security problems (*e.g.,* recovering from extensive compromise, detecting polymorphic attacks, composing security systems) are growing more complex.

Such training requires hands-on experience with secure systems concepts, methods, and tools, yet many institutions of higher learning lack the resources to provide that experience. Even large universities often lack the facilities and expertise to expose students to the thorny details that crop up when trying to address these types of challenges.

Although other efforts both inside and outside the formal classroom structure to provide hands-on information security work exist [6, 5, 7], we felt that there was still tremendous need for innovative programs in this space. We created the SISMAT (Secure Information Systems Mentoring and Training) program to combine research, training, and outreach efforts in information security. The main purpose of SISMAT is to nurture security expertise in current undergraduates while supporting faculty members in their development of curricula that will enable future generations of students to confront these information security challenges head-on. Increasing the availability of educational opportunities for undergraduate students, particularly those that attend colleges without a strong systems or security research lab, is one way in which we can help build the nation's capacity for cyber security expertise.

SISMAT's core is a summer training program to help undergraduates from around the country receive in-depth training in specific information security topics. SISMAT is not just a summer "security camp"; it also seeks to mentor participants and their academic advisors during a related summer internship in industry (or non-profit organization) and subsequent research project during the following school year. This arrangement benefits the students, the internship partners, and helps to create a broader research and education community around infrastructure security concerns.

1.1 Vision

Our primary purpose in writing this paper is to share a model of a successful education and outreach program (and the reasons for this success) in hopes of creating similar concerted efforts throughout the country. We hope that SISMAT can be a model that may be adapted to work at other institutions. In particular, we wanted to use our expertise in very specific information security topics to create something different and more valuable than just a summer "security boot camp." We did not plan a broad summer school (in the spirit of NSA COEs) that provided a comprehensive look at an entire field, but rather we designed a tightly focused project based on our specific areas of expertise. We are confident that a few focused researchers could use this

ACEIS '09 Ames, Iowa USA

model to create a similar program at another university.

As noted in the introduction, much of the inspiration behind SISMAT came from wide pressure to protect our nation's public and private information infrastructure against increasingly sophisticated cyber threats. Institutions across the country are clamoring for skilled workers trained in cutting–edge cyber security tools (and, perhaps more importantly, for workers who can create and enhance such tools). Even large companies with well-established human resources departments have difficulty finding qualified individuals; one commercial SISMAT partner expressed their frustration with the inability of the current recruitment infrastructure to even identify suitable candidates. Given how many different organizations were experiencing similar trouble, it became clear to us that the traditional training and hiring pipeline is not meeting the modern need for information security professionals.

Because many different communities share this challenge, we founded our effort on the formation of flexible mentoring and training partnerships that span community boundaries. We envisioned a program with three principle components: first, we would offer an intense, vigorous, and in-depth two week training program in specific information security topics (chosen based on our our expertise and the expressed needs of our public and private sector colleagues) for undergraduates. Second, we would link these students with a practical, hands-on internship experience in information security and assurance. Finally, we would support a mentored research project for each student at their local academic institutions, in cooperation with that institution's faculty.

Most immediately, this structure enabled us to offer undergraduate participants with training not offered at their own schools. The internship component matched the participants with commercial and governmental entities that have a difficult time finding qualified security professionals. Finally, the mentored research project allowed us to assist the development of security education by offering ongoing mentoring and community-based resources to faculty members.

By working with industry partners and faculty and students of other academic institutions, we hoped to foster improvements in cyber security education and provide undergraduates with valuable experience developing and maintaining secure information infrastructure. As such, our goals included:

1. **Mentoring and Training** to help talented but underserved students in specific cyber-security topics, particularly PKI, penetration testing, and intrusion defense analysis, topics that we have specific expertise in.

2. **Develop Curriculum** by encouraging research and development in secure cyber infrastructure at our partner institutions via mentored research projects.

3. **Increase Participation** by providing opportunities in secure systems research to traditionally underrepresented populations (we recruited heavily from women's colleges and small public institutions).

We chose the structure of SISMAT to overcome critical barriers for selected student communities. Securing cyber infrastructure requires hands-on experience with real systems. Students at many smaller colleges, however, do not have the opportunity to easily get this experience. Furthermore, venturing into the cyber security classroom and workforce — typically dominated by "alpha-geek" males — can be intimidating for students who do not fit this model.

Not only do the goals of SISMAT align well with existing commercial needs, research goals, and governmental cybersecurity priorities, but SISMAT, and the subsequent ideas it has inspired, represent a novel paradigm for sustainably meeting these needs, goals, and priorities as they rapidly evolve in the future. In this way, SISMAT can help construct these conduits of information from "real world" security practitioners to the academics who develop undergraduate security curricula.

1.2 Paper Organization

This paper offers detailed information on the development and implementation of SISMAT. In this section, we introduced our motivation and the need for a program like SISMAT. We also provided an outline of the broad structure of the program itself. Section 2 provides a detailed overview of SISMAT, including topics covered and lab exercises. Section 4 contains participant feedback.

We note that in order to conform with the ACEIS call for papers, we have anonymized the paper to remove explicit references to our institution and partners, but we recognize that a simple Web search for the name of the program itself would partially de-anonymize our organization and some of the authors.

1.3 Major Observations

Throughout the paper, we highlight some of the most novel aspects of SISMAT and the interesting lessons that we have learned from designing and running the program. We summarize some of the most interesting points here.

1.3.1 Program Structure

We believe that the structure of the SISMAT program is of interest because it is *comprehensive*: it addresses three complementary educational aspects. First, the core educational component combines a deep training experience with a small "class" size and one-on-one attention from instructors. Second, SISMAT provides the student with the opportunity to enhance these skills in a real-world environment with a paid internship related to information security. Finally, it encourages the student and their faculty mentor to use these experience to adopt, design, or develop information security concepts into their local curriculum. The combination of training, internship, and mentoring components offer participants a holistic educational experience; both students and faculty who complete the SISMAT program have an up-to-date understanding of information security problems, and are empowered to delve deeper into the research, education, and practice of the field.

1.3.2 Interactive Curriculum

We employed a wiki to list the day-by-day and session-by-session curriculum for the course component. We dynamically updated the links, topics, and supporting materials based on interaction with the student in the labs and lecture sessions. Each day, we posted links that would be useful for the lab sessions, and we also posted links to homework readings, papers, and Web sites.

The wiki turned out to be a fantastic resource, especially

for the students: they had full permissions to modify the wiki pages and often did so to post resources they had found on other websites. During some of the lab exercises, we also asked them to post various files (*e.g.,* access permission records, `passwd` files). The wiki served to increase the interactivity between the students, the instructors, and their faculty mentors. The wiki served as an organic record of an ongoing conversation between these principals. While educators can sometimes struggle to adapt pre-existing "course management" systems like Blackboard into the classroom (and students often meet these efforts with skeptical indifference), we were pleased to see this single relatively unstructured wiki used so well. Further experience may reveal which aspects of the SISMAT curriculum or environment made this collaborative technology successful for program participants.

1.3.3 Ethics Discussion

We planned a discussion of information security ethics at the *end* of the education component rather than the beginning. Students noted that such a discussion would lack detail at the beginning of the workshop. As such, it would have mostly focused on emotional argument that would have been forgotten in the course of the workshop rather than informed debate that could leave an impression immediately after the workshop.

1.3.4 Logistics

One valuable *practical* result of having run a pilot version of SISMAT is that we have a clear idea of the costs, time, equipment, and personnel required to execute such a program. We look forward to helping other cyber security training efforts by providing them with the benefit of our experience, and we are happy to share this knowledge. This paper is, in part, a manifestation of that type of effort.

2. OVERVIEW AND STRUCTURE

SISMAT aims to connect and foster relationships among security researchers, commercial and governmental organizations, and the faculty and students of undergraduate institutions with underdeveloped computer security curricula or expertise. We target colleges whose curricula will have prepared upper-level undergraduates for this hands-on work but cannot offer it themselves[1]; we target cyber security focus areas in which we have local leadership and expertise; and we target external partners that have communicated a need for training in these areas. We next provide an overview of the three phases of SISMAT: an intensive two-week seminar, internships, and a mentored research project.

2.1 Phase I: Training

This pilot version of SISMAT enabled us to formulate processes for identifying, recruiting, and housing students. We provided housing and meals for the students we recruited, along with travel costs, for the two-week seminar. We had roughly fifteen applicants and selected seven from this set. Our aim was to keep the program small and provide one-on-one attention during this pilot version of the seminar. We provided the students and their faculty mentors with copies (theirs to keep) of three popular texts in the information security field: "Applied Cryptography" [8], "The Craft of System Security" [9], and "Network Security: Private Communication in a Public World" [3].

We also created a set of training material and a program of guest speakers for the seminar. This training curriculum structure (and the accompanying content) has helped achieve the educational goals of our program: (a) enable students to gain traction in some key areas (PKI, penetration testing, ethics, network intrusion response) in demand by industry, government, and academia; (b) supply faculty members with a strong foundation for a semester-long course; and (c) create an artifact that we can share with the wider security education community. The major topics covered in the course are shown in Table 2.1.

2.1.1 Day Structure

We structured each day of the SISMAT two-week seminar to be a full day of lecture and lab work, with timely breaks. Each day started at 8:30 AM and typically lasted to 6:00 PM (although the students sometimes stayed well beyond this "formal" end of the day to work on lab exercises that really engaged them). The days are split between two morning lectures (which were sometimes full lectures and sometimes talks given by guest speakers) and two afternoon labs. We left significant time for a midday break for the students to recharge, and we inserted smaller breaks in between the morning and afternoon sessions. We assigned readings every night to reinforce the topics covered that day and preview topics for the following day.

The small, focused, and intimate nature of the labs and lecture allow for more leisurely exploration of corner cases and difficult concepts [4]. The material that we fit into these two weeks approaches the material for a semester-length course; because we spend significant amounts of time delving into details, this mapping is not straightforward, but rather an approximation.

2.1.2 Labs

We used a dedicated computer laboratory for the afternoon exercises. The room was equipped with a Linux workstation for each student, a projector, a custom-designed and isolated network, whiteboards on the opposite wall for group discussion, and rolling office chairs to allow students to quickly change physical configurations as the various activities warranted. In presenting each exercise, we strove to create an atmosphere of collaborative experimentation, rather than classroom instruction. Although we provided background information as necessary, we knew that students would soon be immersed in a variety of internship tasks, and thus asked them to practice their communication and curiosity as much as their technical problem-solving skills.

We planned a number of lab exercises for the students. Each day had time slots for two separate (in practice, related) lab exercises or demo sessions. Some of the highlights of these exercises (from the student's perspective) include:

1. practicing HTML, Javascript, and SQL injection attacks
2. walking through the OpenSSL "roll-your-own CA" exercise
3. forging and digitally signing email from an entity that shared the same identifying information as our University President (as a practical illustration of the need

[1]We were inspired to create this program because of our direct experience in this type of educational environment.

Table 1: *SISMAT Seminar Topics.* Each topic maps roughly to a day in the two-week seminar; given the inclusion of guest speakers, a day of introduction to the Linux environment, and some topics being split across days, this program content fills the two week (10 business days) seminar period.

Topics	Details
Web Vulnerabilities & Injection	HTTP and browser/server interactions, XSS, SQL injection, and countermeasures
Public Key Infrastructures	Basic cryptographic principles, certificates
IT Security Operations	Guest lectures about the operational aspects of PKI and Medical IT infosec
Network Analysis	TCP/IP networking, tcpdump, wireshark, packet crafting, the SSH protocol
Intrusion Detection & Network Mapping	NIDS background, Snort, nmap, and anomaly traffic classifiers
Software Vulnerabilities	Buffer overflows, debugging, real vulnerabilities and exploits, countermeasures
Authentication	Unix groups and permissions, ACLs and capabilities, trust in identity, PKI
Policy & Ethics	Ethics of various information security topics, Java 2 policy

for a process to surround the use of PKI — digital certificates will happily attest to the integrity of falsified information)

4. a detailed, step-by-step analysis of the bash history and log files from a real intrusion incident (utilizing the vmsplice vulnerability) into a server running a MySQL database, including all downloaded scripts and source code for an IRC fuzzer as well as the vmsplice exploit source code.

5. debugging and analysis of the libpng [1] and nullhttpd [2] vulnerabilities

6. an exercise dealing with authorization policy in the Unix file system set up as a "customer requirements" meeting.

The SQL injection exercise was extremely popular with the students; it was their first lab exercise, and we provided a graduated sequence of tasks that got progressively harder. The final task, we were fairly certain, was impossible to complete with the way we had constructed the Web application and database. To our great delight, however, the students spent a great deal of effort trying to achieve this goal and discovered a number of other information gathering and SQL injection attacks that would have proven useful to accomplishing the final task.

The students also had a tremendous amount of fun in the forensic exercise of analyzing the real intrusion incident. For many of them, it was the first time they had the opportunity to look at the actual remains of a server after it had been compromised. Reconstructing the attacker's timeline was particularly entertaining. Without very little prodding, the students were able to observe several things about the attacker and hypothesize that they were most likely a script kiddie rather than an accomplished hacker. Even so, the exercise showed how powerful a few pre-packaged tools and exploit code could be even in the hands of the less accomplished.

Designing rewarding academic exercises in cyber security requires both technical knowledge and creativity; teaching the SISMAT labs also required rigorous time management, adaptability, and patience in working with the same students for two weeks straight. Leading the exercise on access control, for example, was both challenging and rewarding: we wanted to acquaint students with the related concepts that are ubiquitous in computer security, but not get mired too deeply in any particular approach; we wanted to familiarize them with access control lists, permission management, and policy definition, but also keep the students engaged and technically challenged.

2.1.3 Guest Speakers

We felt that exposing the students to a variety of guest speakers was a vital way to keep the program exciting and interesting: two full weeks with only a single instructor (one of the authors) could become quite a drain both on the instructor as well as the students. To this end, we included, besides the main instructor, five guest speakers.

- We asked an NSA employee to speak with the students about information security jobs, particularly in the US Government.

- We invited an independent information security consultant and a co-author of one of the texts used in the seminar to speak about his experiences as well as aspects of software attacks.

- A member of our IT staff and recognized PKI expert guided the students through the basics of PKI. He also gave them a talk on his practical experiences with PKI and a tour of our IT machine room.

- We invited the head of IT Security (coincidentally, one of our internship mentors) for our affiliated medical school to give a talk on the intersection of information security and the health services field.

- Finally, a PhD student (one of the authors), provided the participants with a fascinating look at current large-scale distributed authentication and authorization policies. The student also led a lab session dealing with the surprising challenges of crafting authorization policy in the Unix system.

2.1.4 Mentor Development Weekend

The SISMAT program included a weekend "professional development" workshop for the faculty mentors of the SISMAT participants. This weekend was hosted by the authors and instructors, and it included a guest talks by two local undergraduates and one of our IT Security employees. During this weekend workshop, we discussed strategies for teaching information security topics with the faculty mentors, shared details of our CSI (Cyber Security Initiative, a joint program between our Department and IT Services that encourages "ethical hacking" by supervised undergraduates), and offered an opportunity to discuss successful undergraduate mentoring with former Women in Science Project (WISP) interns of our lab.

One theme that emerged from this weekend was the lack of a good channel for academics and industry leaders with information security expertise to transfer their knowledge,

curriculum material, and pedagogy to other academics. This lack seems to present a striking opportunity to coordinate members of SIGCSE and SIGSAC (and similar communities) to help create such a channel. We were happy to discover the existence of ACEIS, as we believe it is a perfect venue for encouraging and fostering this type of exchange. We envision drawing on members of SIGCSE who have traditionally worked on bringing security-related material into their local curriculum and members of the computer security research community who have the time and talent to contribute to fortifying the wider security curriculum.

2.2 Phase II: Internships

We identified a number of internship opportunities for the SISMAT participants. One challenge we faced was in matching students to internships while facilitating a mutual vetting process of the parties involved. We arranged internships at a governmental PKI authority, a financial services company, a large defense contractor, a large university, a hospital and medical center, and our institution's IT and computing services. One major feature of our program was to offer a stipend for students undertaking internships at non-profit organizations: such organizations often have interesting security problems to solve but little resources to address them. In addition, we offered notebook computers to help support these students during their internships.

2.3 Phase III: Research Projects

The final important aspect of SISMAT is a research project undertaken by the participants under the guidance of their faculty mentor and with the ability to consult us for technical support, suggestions, and resources. We envisioned such projects to include both curriculum development efforts as well as more traditional information security projects.

We, in conjunction with the SISMAT participants, created a list of projects that involves vulnerability analysis, tool building, authorization policy enhancements, and curriculum development topics. This project list includes topics like developing system call fuzzers, updating a password cracker to handle SHA-256 password encoding, creating browser plugins to display a protocol ladder diagram, assessing the security of a Medical Records System, and extending Java 2 Policy and Permissions to handle temporal logic and privilege drop. It also includes possible curriculum development ideas like creating an introductory course in Information Privacy and Ethics, developing exercises for an undergraduate networking or algorithms course that shows how spanning tree and shortest-path algorithms operate when nodes behave in an adversarial way, and developing a grid computing course that compares the use of different PKI solutions to distribute, run, and revoke tasks.

We are in the process of setting up infrastructure for the storage, maintenance, and annotation of a repository of student projects. This repository will serve the wider academic community as a resource for project ideas (to continue or enhance some of the existing projects) as well as course material. These projects are merely representative samples of material that might reside in such a repository. For now, students and their faculty mentors are keeping track of their own progress using their local institutional resources; we hope to offer them a svn, wiki, blog, and web access to the repository site hosted at our institution; we would be responsible for curating and managing this collection. A repository would provide a tangible collection of artifacts; a carefully curated collection supplies the cyber-security education community with a well-maintained resource and a legacy that directly illustrates the growth and maturation of cyber-security education.

3. EXPERIENCES, OBSERVATIONS, AND OUTGROWTH

Designing and running the pilot version of SISMAT required a significant amount of effort from personnel at our institution. We feel, however, that this program is well worth that effort, especially since we can take advantage of the processes, infrastructure, and relationships we have already developed during the course of the pilot year. We have found ourselves energized by the program and our interaction with the student participants and faculty mentors.

As researchers and educators, we have derived two major benefits from designing and running the pilot version of SISMAT. First, we have been able to create and adjust a curriculum structure (and the accompanying content) that achieved the educational goals of our program: (*a*) enable students to gain traction in some key areas (PKI, pen testing, ethics, network security) in demand by industry, government, and academia, (*b*) supply faculty members with a strong foundation for a semester-long course, and (*c*) create an artifact that we can share with the wider security education community.

Aside from the educational benefits, the second major benefit of designing and running the SISMAT program has been an almost purely logistical one. The investment of time, effort, and our current funding has augmented our understanding of where the pitfalls and obstacles are and how to avoid them. This is not to say that the topics we mention below did not go smoothly, or that major problems existed; rather, the experience has provided us the opportunity to observe what works well and how we might tweak the process to improve its efficiency.

In particular, we gained experience in recruiting and housing students, and we have a detailed understanding of the requirements and process of organizing, ordering, and configuring lab workspace and equipment. We have been able to gauge the time needed by various actors to contribute to portions of the project, including a project lead, lab supervisors, support staff, guest speakers, and guest instructors. We expect that the roles required to execute SISMAT can be found within most academic organizations. In addition, the program has served to strengthen our relationships with both area colleges and a variety of industry, government, and non-profit organizations. Strengthening these ties is an important outcome because it enables us to not only ramp up the SISMAT program, but also creates opportunities for our partner colleges to interact and grow *their* relationships with industry, government, and non-profit organizations.

3.1 Outgrowth

As we reviewed our engagement with SISMAT, we were excited at the opportunity to leverage our experience in a number of ways. First, we see the possibility of scaling up the program to include more schools, participants, and internships. Second, having designed a detailed but flexible curriculum structure, we see several ways that we can modify the curriculum and augment the lab experience with ad-

ditional infrastructure and lab exercises. In particular, we plan to move the exercises to a virtual machine infrastructure for easy setup, backup, and storage. Such an undertaking has the twin benefit of making it easy to share the lab material and replicate SISMAT at other institutions.

3.1.1 Alternative Outreach

We would like to see the benefits of SISMAT go beyond our institution and current set of SISMAT partners. We believe that a unique opportunity for complementing grant proposals exists. Grant proposals often include an outreach component; oftentimes this component contains boilerplate text proposing to transfer parts of the research program into some subset of the local undergraduate or graduate curriculum. Such an effort can be difficult to achieve, especially at institutions without a strong security curriculum: there is literally no place to transfer research-level security knowledge into course material. Even at institutions with well–established security research and course tracks, it can be difficult to translate novel research papers into course material.

We believe that SISMAT presents an exciting alternative model for outreach components of grant proposals. Since we can estimate what a SISMAT participant or guest speaker might cost (travel, lodging, meals, books, equipment, potential stipend at a non-profit), grants can include funding for students to attend future SISMAT seminars, funding for an undergraduate student (much like NSF REUs) from another college to undertake an internship in the local environment (assuming the local environment has a strong security research program), or funding for advanced graduate students to participate as guest speakers in a SISMAT program.

4. FEEDBACK

Aside from the benefits to us as researchers and educators, SISMAT has been particularly successful from the point of view of the student and faculty participants: the purpose of the entire program. Rather than impose our editorial voice on the views of the participants, we next include quotes taken directly from the feedback we solicited during and immediately after the SISMAT workshop conclusion as well as a hot wash session during the last day of the program. The feedback we have had was overwhelmingly positive. In addition, all the participants in the professional development weekend were inspired by the retreat-like atmosphere and the possibility of breaking this component out to a seminar-style meeting where the participants (both faculty and students) could concentrate on curriculum development, project ideas, and feedback.

4.1 Student and Faculty Comments

In general, the students enjoyed the structure of the day; although each day was full (2 lectures and 2 lab exercises taking from 8:30 AM to an average of 6:00 PM), the day was structured well enough to provide breaks for the students to recharge and relax. The students enjoyed the readings (and were uniformly engaged in undertaking them, even when they introduced unfamiliar or difficult topics like arguments about the utility of PKI, which require a certain level of expertise with PKI basics).

The students also highlighted several areas for improvement, including having a social activity to start the week in addition to an outing in the middle of the program. Suggestions included viewing classic hacker movies (*e.g.,* War Games, Sneakers, Swordfish, Hackers): an occasion that could be followed by a discussion of how realistic these depictions are.

> *"I had a great time last week as part of the SISMAT program...the traveling up here and moving into housing were well handled. The talk by Doug and Scott on what their work involves was a great eye opener. They supplemented the lectures well."*
>
> *"Though the first couple of labs turned out to be long, I learned a lot. Through the work we are doing, i am actually starting to take time to read manuals!"*
>
> *"I want to start by saying that overall everything and everyone has been great and very helpful. You guys definitely did a great job of making sure everyone had everything they needed."*
>
> *"When it comes to the readings/lectures/labs, I think it shows that a lot of time also went into preparing these as well. I enjoy them and think I am learning a lot."*
>
> *"I enjoy being a participant in the 2008 SISMAT program. I like everything about this program including the way it is structured..."*
>
> *"One thing that would be useful would be a time for all of the students and mentors to get together and talk about project ideas. The mentor project seems a little disjoint from the rest of the SISMAT program, and I think this would help tie them together."*
>
> *"I found that it was a good idea to give a brief introduction about the topics that we were talking about that same day or the night before with the readings."*
>
> *"I like how the tasks of the labs are set up and are designed with exercises that range from easy to hard in there difficulty. I liked how the labs sometimes were not just straight forward and easy to do."*
>
> *"If I would add anything to the program I would suggest that there be a lecture dedicated to and talking about graduate school. Graduate school degrees seemed very relevant and it was something that every one of the speakers had in common with each other."*
>
> *"I was very impressed by the breadth and depth of your knowledge of security and learned a lot from you...you put together a dynamite boot-camp course for the students, and I will be reviewing your syllabus carefully in planning my security course this Fall."*

These quotes reflect our commitment to help students explore the corner cases of a system or problem for a more complete understanding of the space where software and conceptual design flaws and faults live — a process that is not typically reflected in undergraduate course curriculum that usually focus on the "success path" or main case of a tool, language, API, or algorithm.

5. CONCLUSIONS

SISMAT is an ambitious information security education and training program for undergraduate students consisting of three major components: a training program, an internship, and a mentored research project to help spur the growth of security curriculum at the participating schools. As researchers, educators, and computer scientists, we believe that programs like SISMAT are invaluable for helping fulfill the national educational and outreach missions of the National Science Foundation and the cyber-security education mission of the Department of Homeland Security.

Programs like SISMAT help increase the availability of educational opportunities for undergraduate students, particularly those that attend colleges without a strong systems or security research presence. SISMAT directly engenders a pipeline of knowledge from security researchers and industry experts to the SISMAT faculty mentors, who can then weave this knowledge into their local curriculum. One of the most important aspects of programs like SISMAT and conferences like ACEIS is to help foster an exchange between communities like SIGSAC and SIGCSE.

Acknowledgments

This paper results from a research program in the Institute for Security, Technology, and Society at Dartmouth College, supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001. Locasto is supported by the Institute for Information Infrastructure Protection (I3P). The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

6. REFERENCES

[1] `http://www.us-cert.gov/cas/techalerts/TA04-217A.html`.

[2] `http://www.securityfocus.com/bid/5774`.

[3] Kaufman, C., Perlman, R., and Speciner, M. *Network Security: Private Communication in a Public World*, 2nd ed. Prentice Hall, 2007.

[4] Knox, D. L., DePasquale, P. J., and Pulimood, S. M. A model for summer undergraduate research experiences in emerging technologies. *SIGCSE Bull. 38*, 1 (2006), 214–218.

[5] Logan, P. Y., and Clarkson, A. Teaching students to hack: curriculum issues in information security. In *SIGCSE '05: Proceedings of the 36th SIGCSE technical symposium on Computer science education* (New York, NY, USA, 2005), ACM, pp. 157–161.

[6] Mateti, P. A laboratory-based course on internet security. In *SIGCSE '03: Proceedings of the 34th SIGCSE technical symposium on Computer science education* (New York, NY, USA, 2003), ACM, pp. 252–256.

[7] Pashel, B. A. Teaching students to hack: ethical implications in teaching students to hack at the university level. In *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development* (New York, NY, USA, 2006), ACM, pp. 197–200.

[8] Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc.

[9] Smith, S., and Marchesini, J. *The Craft of System Security*. Addison-Wesley, 2008.