Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Implementation and Lessons Learned from an Undergraduate Special Interest Group in Information Assurance

Gregory Conti, Daniel Ragsdale, Scott Lathrop and Christopher Gates

Abstract – This paper describes the methodology, implementation and results from the formation and execution of an undergraduate information assurance student group. In February 2001, our institution formed a student chapter of the Association for Computing Machinery's Special Interest Group for Security, Audit and Control (ACM-SIGSAC) due to extensive interest by the student body in computer security and information assurance, as well as an awareness of the critical need by the faculty. This was the first information assurance student chapter formed out of the more than 600 ACM student organizations worldwide. The chapter was formed with an interdisciplinary approach in order to include a larger portion of the student body and thus influence a larger audience. This approach proved successful. Over the past three years, the group has grown from an idea to a vibrant organization of approximately 600 students. We believe that we have struck a chord with the students that merits examination. The primary goal of this paper is to provide a descriptive resource to educators who wish to implement a student information assurance group. It includes the purpose and methodology behind the formation of the group, our successes and failures, our lessons learned, and potential future directions.

Index terms – information assurance, information assurance club, interdisciplinary information assurance, computer security club, information assurance student chapter, SIGSAC

I. Introduction

This paper describes the methodology, lessons learned and results from the formation and three-year execution of an undergraduate information assurance student group. In February 2001, our institution formed a student chapter of the Association for Computing Machinery's Special Interest Group for Security, Audit and Control (ACM-SIGSAC) due to extensive interest by the student body in computer security and information assurance as well as an awareness of the critical need by the faculty. This was the first SIGSAC student chapter formed out of the more than 600 ACM student organizations worldwide.

The chapter was formed with an interdisciplinary approach in order to include a larger portion of the student body and thus influence a larger audience. The first SIGSAC meeting was held in February 2001 and was attended by approximately 80 students. Since that time, membership has dramatically expanded and, as of Spring 2004, we appear to be at a stable state of approximately 600 members. This number is quite significant in that it exceeds 10% of the student body and particularly when compared to the institution-wide population of approximately 78 computer science majors. We believe that we have struck a chord with the students that merits examination.

The primary goal of this paper is to provide a descriptive resource to educators who wish to implement a student information assurance group. It includes the purpose and methodology behind the formation of the group, the lessons learned, and potential future directions for research. It is our sincere hope to inspire and aid others in starting similar organizations, but we fully understand that each educational institution is unique. To this end, we have included broader techniques that can be tailored to most other academic institutions. We believe these techniques will scale from small informal groups to large well-resourced organizations.

II. Background and Motivation

Why form such a group in the first place? What are the benefits? These questions are an important part of the discussion and must be answered when considering the formation of a student information assurance group. The answers fall into several major categories:

- Increase information assurance awareness across intellectual disciplines
- Complement the formal information assurance educational program
- Provide ethical education and reinforcement of positive values
- Foster information assurance discussion and debate
- Contribute to the computer science and information assurance professions

Regardless of whether you choose to create such a group, we argue that these are goals worthy of pursuit.

ISBN 0-87145-192-1/04/$15.00

A. Increased Information Assurance Awareness

A student organization can increase awareness of information assurance across many levels. At the most basic level, the activities of such a group can increase awareness of the general principals of information assurance across a broad swath of an institution's student body, faculty and staff, as well as increasing the exposure of professional societies such as the Association for Computing Machinery (ACM) and the ACM's Special Interest Group for Security, Audit and Control (SIGSAC). These general principals include the understanding of the potential threat to national security and personal privacy as well as to encourage good information security practices. The interdisciplinary approach was utilized to reach people outside the traditional computer science community by including appropriate political, economic, social, ethical, legal, and technological coverage. Beyond basic understanding, the group included applied training and education across the spectrum of information assurance.

B. Complement Formal Educational Program

Formal classroom education is a powerful tool, but is limited, to some degree, by the four walls of the classroom. A properly formed information assurance club can increase awareness and generate enthusiasm for learning that complements and reinforces the classroom experience. The interdisciplinary nature of such a group reaches beyond the traditional boundaries of computer security to a much wider audience, such as law and international relations majors, to impress upon them the importance of information assurance. Beyond student clubs, more information on a comprehensive undergraduate information assurance program can be found in another paper.[1]

C. Ethical Education and Reinforcement of Positive Values

The information assurance domain is fraught with risks. Both students and faculty will face ethical questions about the appropriate and inappropriate use of technology. A student club of this nature provides ample opportunity to teach, reinforce and apply ethics. An excellent starting point is the ACM Code of Ethics and Professional Conduct.[2] In addition, our institution's honor code provides guidance for our student body. The combination of these ethical codes could help to demonstrate the larger professional and academic importance of ethical conduct with respect to information assurance. A related benefit of this group is that it will help the students form an association with the "white hat" information assurance profession early on in their careers. Finally, this club will help harness interest and focus it into healthy areas.

D. Foster Discussion and Debate

There are often no clear answers to information assurance related questions. A student club can provide a forum for discussion and debate and could increase interaction between students, faculty, the local community, academia, government and business. A multidiscipline approach fosters multidiscipline interaction with potential for increased crossover of benefits from the traditional computer science field to a much larger arena. This arena composed of students, faculty, the local community, academia, government and business can develop a broadened and enriched image of computer science and information assurance. An additional benefit is that discussion and debate will help faculty members identify appropriate students for individual research, summer internships, information assurance courses and related conferences. The club would also provide a pool of students and faculty to explore new ideas on a much more focused footing.

E. Contribute to the Computer Science and Information Assurance Professions

A properly constructed information assurance club can create agents of change; students and faculty who truly understand the importance and potential risks associated with information assurance. With an expanded membership far beyond traditional boundaries these lessons will impact a much larger audience. It will also provide positive exposure of professional societies, such as the ACM, and the field of computer science.

III. Related Work

The uniqueness of this paper springs the real-world lessons learned from a large-scale, long-term implementation of an undergraduate information assurance club. There is a limited body of related work in the area of undergraduate information assurance student organizations. Multiple institutions include some degree of computer security as part of an undergraduate computer science club. For example, Colorado State University's ACM chapter includes among its previous activities, a presentation on hacking as one of the benefits of joining.[3] Unfortunately, only a small number of academic institutions have taken steps toward a specialized organization. As of early 2001, the Association of Computing Machinery had over 600 student chapters worldwide, but none dedicated to information assurance. In a paper presented at the 2002 National Colloquium on Information Assurance Education (NCISSE), Hintz from the University of Texas at Austin proposed the formation of such groups.[4] It is worthwhile reading that provides valuable insight into forming a group from a student's perspective. Iowa State University is forming an Information Assurance club.[5] Grinnell College has a

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Whitehat Hacking Club designed to "raise awareness about network security and the Internet, teach use of free software, demonstrate good computer ethics, present Hacker pop culture/eliminate Hacker myths and teach people to be more responsible Internet users."[6,7]

IV. Risks

Information assurance is a double-edged sword. The knowledge to protect information is entwined with the knowledge to do harm. There are several risks that lie in forming a group that studies the defense of computer systems by learning their weaknesses. Of primary importance is the fact that we did not want to create an ethical monster. To quote our Dean, he did not want to "create the next generation of hackers." Our plan included support from our institution's Information Technology and Operations Center (ITOC) research group and their Information Warfare Lab (IWAR). The IWAR lab is a completely isolated network that allows use of security and hacking tools in a safe environment.[8] If a student leaked a tool from the lab and used it on the campus network, the entire organization would be put at risk. Worse yet, the student could use their knowledge to attack a computer external to the institution. It is possible to imagine a whole host of legal ramifications and bad publicity that one could encounter if the students were not properly restrained.

Other, more administrative concerns included the cost of ACM and SIGSAC memberships and space for meetings. These risks, balanced against the benefits, dictated how the group was organized from the very beginning. Senior departmental and institutional leaders as well as the Institution's legal office were consulted to garner support, guidance and advice. Other specific measures undertaken to mitigate these risks are woven into the following discussion.

V. Methodology and Results

A. Initial Organization and Administration

A club requires members. We sought to form a group which, as its primary mission, taught information assurance and at the same time was fun for students. We made the conscious decision to introduce the club to the students as an "information warfare" club and to make minimal use of the somewhat unwieldy, term ACM/SIGSAC. Later, as students became familiar with the club, we provided more exposure to the terms ACM and SIGSAC and their role in the computer science communities. This proved to be successful. Once students became active with the club they were introduced to the deeper concepts involved beyond the glamorous term of information warfare.

The promotion of the club included a variety of activities:

- A demonstration of computer security tools in the institution's core (required of all students, regardless of major) information technology course (IT105) followed by the distribution of club literature. The tools included a demonstration of the Sub7 trojan. This briefing is now a permanent fixture of the course and reaches virtually 100% of each freshman class annually. This event is further reinforced by IT105 instructors who promote the group during a separate lesson on information warfare.
- The creation of an email distribution list to disseminate breaking news in the information assurance field and as a means to distribute information on club activities. The club members would forward these emails to other interested students and helped facilitate the rapid growth. The volume of email was carefully managed so as not to deluge the members with excess mail.
- Flyers posted to the Electrical Engineering and Computer Science departmental bulletin boards.
- The advertisements included notice of upcoming meetings, speakers and trips. They also included promotion of club member access to the IWAR lab.
- A club website with a database of members.
- Selling the benefits of ACM and SIGSAC professional society membership.

Marketing served as both a means and an end. It attracted new members, while at the same time, spread the word about information assurance. Leaders felt it important to set the tone that this was not a hacker club, but one dedicated to information assurance.

These activities got the word out and approximately 105 students participated in the initial meeting. This initial meeting consisted of brainstorming future activities, an overview of the ACM/SIGSAC and laying the groundwork for the election of officers. To enhance the upbeat nature of the group we played techno music as students entered the meeting as well as provided pizza. At this first meeting faculty members made it clear to the students that this was not a "hacker" club, but instead a club dedicated to learning about information security. Sign-in sheets were used to document those who attended.

The club's rapid growth demanded active student leaders and faculty advisors. We conducted an initial election in March 2001, electing a chair, co-chair, activities chair and secretary/treasurer. They, in turn, built the infrastructure to handle the large growth including a database of membership information, club website and email distribution list. The leadership placed significant priority to activities and recruiting.

Beginning with these initial organizational activities, faculty members and student leaders took advantage of the substantial support the ACM provides for student chapters. The student chapter start-up kits, brochures and posters made the

administrative requirements of starting a chapter very straightforward. In particular, the ACM's student chapter support website provided examples of the bylaws, charter and petition required to formally instantiate a chapter. They also require that the primary student leaders and faculty advisor be members of both the ACM and the respective Special Interest Group.

In the next year, growth within the club was dramatic. In order to cope with this dramatic growth in membership, faculty advisors and student leaders used a variety of techniques. First and foremost, a spreadsheet was essential to track membership information and event participation. Email distribution lists were the primary means of distributing membership information. In particular, the voting button capability provided by Microsoft Outlook proved to be essential for determining student interest for each event. The email lists were augmented by the group website which provided less time critical information. The website was divided into four main areas:

- About SIGSAC and the ACM
- Activities (both planned and historical)
- Leadership
- Information assurance web links

Finally, as the membership roster grew to include over 450 members, the initial student leadership team was severely taxed. This was mitigated by the recruitment of additional students to serve as event coordinators and proved to be particularly successful when the volunteer was personally interested in the event. A good example is of a student majoring in law who volunteered to organize a visit by a local district attorney planning to talk about prosecuting cybercrime. This technique helped, but certain leadership positions, especially the secretary and club president, were still in danger of becoming overwhelmed. Faculty advisors helped to relieve this situation during the March 2002 election by expanding the leadership structure of the group to include:

- Chair
- Co-chair
- Activities chair (local events)
- Activities chair (trips)
- Secretary
- Assistant secretary
- Freshman liaison
- IEEE liaison
- IWAR lab director
- Assistant IWAR lab director

The division of the activities chair role reduced the burden of event planning and the assistant to the secretary helped minimize the administrative bottleneck. The freshman liaison provided a voice for the new students and helped to plan several highly successful freshman-only events. The IEEE liaison was the Chair of our institution's student IEEE chapter and helped coordinate joint functions. Three new faculty members were also recruited to serve as advisors and to provide continuity as some faculty departed the institution.

B. Activities

1. Overview

Central to the success and rapid growth of the group was an exciting set of activities. The diverse nature of the group demanded a wide variety of events designed to reach across many disciplines. These activities were divided into several categories: guest speakers, meetings, conferences, LAN parties, community service, trips, short courses and creation of an information warfare lab.

The most successful aspect of the chapter's activities was the guest speaker program. Representative speakers included:

- A Steganography Expert
- A Corporate Information Security Red Team
- Secret Service Cybercrime Agents
- A military computer crime investigative unit
- Members from the Honeynet project

The first four speakers listed above covered the breadth of academic security researchers, corporate security analysts and government investigatory personnel. It is important to note that the Honeynet project representatives included an eclectic mix of self-taught experts, several of whom had blackhat backgrounds, but had since turned to the legal side of computer security. Their experiences provided a unique forum for discussion about the ethics of hacking from both sides.

Chapter members frequently volunteered to serve as student escorts and informal campus tour guides for the speakers. Based on student input, a well-regarded aspect of the club was the opportunity to interact with the faculty advisors and guest speakers in a non-classroom environment. Feedback suggested that students enjoyed the opportunity to discuss a wide range of career options. Other student feedback stated that the range of talks and trips gave them a wide exposure to the spectrum of jobs in the information assurance field and that "most people would have never known those opportunities existed had it not been for the club."

The chapter was not the primary coordinator for several other speaking events. Cross coordination with other groups across campus allowed for significant synergy. SIGSAC faculty advisors would coordinate with these other groups and ask permission to send members. Without exception, this was warmly received by those organizing the event. Some examples of this synergy include:

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

- World War II Codetalkers by the Native American Club
- Army Deputy Chief of Staff for Intelligence by the Department of Military Instruction
- NSA Overview by the Computer Science Program

Initial work was done to implement a series of short courses on information security topics. A faculty member prepared an hour-long course on physical security using lock picking as the draw for students. Approximately 20 students attended each of three offerings. Current plans include transitioning to student prepared and delivered briefings on cryptographic tools (steganography and public key encryption), open source software and port scanning.

The entire chapter met, on average, twice per semester. The initial meetings of each semester included organizational information and a small presentation. Later meetings included a formal guest speaker. A small student food ration allotment was sufficient to pay for pizza at each meeting. Chapter leaders met occasionally during each semester to assess past activities and plan for the future.

Our institution's Electrical Engineering and Computer Science Department has limited funding to send students to academic conferences and other trips. By careful coordination with the appropriate organizer, faculty advisors were able to procure chapter seats for the Blackhat Briefings, DEFCON, InfoWarCon and the IEEE Information Assurance Workshop as well as a trip to the National Security Agency. Some of these opportunities were from standby seats where SIGSAC members filled last minute vacancies. The IEEE Information Assurance Workshop was run locally and SIGSAC student members were given a waiver of fees by conference organizers in exchange for assistance at the workshop.

The chapter's activities also included community service work. Students volunteered to prepare an educational presentation on web security and safety and give it to local middle school students. Work in this area is ongoing. Another ongoing activity is the procurement and distribution of the National Security Agency's information security poster series to 32 student common areas and over 20 work areas.

The Information Technology and Operations Center (ITOC) is our institution's research center that covers information assurance. They have created an Information Warfare lab with an air-gapped network to support a course in information assurance. They donated space and six machines to build a scaled down version of the IWAR Lab for use by SIGSAC members. In addition, they donated two dedicated machines with a live Internet feed to search for and download tools for use in the lab. Use of the lab requires a safety briefing by a SIGSAC faculty advisor to ensure that proper safety policies are understood and followed. The chapter's IWAR lab director and their assistants are responsible for maintenance of the facility. The ITOC also procured and donated a large number of computer security books to form a lending library in the IWAR lab. Chapter leaders hope that continued use of the lab will provide an opportunity for increased interaction between members in an informal setting.

The addition of a freshman liaison to the chapter leadership proved to be very beneficial. The student organized several freshman-only LAN parties where the focus was on having fun. These events included pizza and an evening of network gaming. Network games included military wargames and hacking-style games. The events were designed to build cohesion between the chapter members of the freshman class. Lesser emphasis was placed on an information assurance agenda at these gatherings.

This wide variety of formal chapter events was supplemented by other synergistic activities. Faculty advisors sought out word on information assurance related courses offered at our institution and helped spread the word. During the first eighteen months of the chapter two new courses were offered, one by the Math Department on Cryptography and another by the Computer Science and Political Science departments on the Policy and Strategy of Cyberwar. The SIGSAC student population proved to be a fertile ground to find interested students. In the Spring of 2001 and 2002, our institution participated in a new program called the CyberDefense Exercise (CDX). The CDX was organized by the National Security Agency. Participating service academies built networks and defended them against attacks by a variety of red teams. The team with the best performance was awarded the NSA Information Assurance Director's Trophy. Chapter members participated in both events and their previous SIGSAC experience contributed to their top performance. As the visibility and importance of the CDX grows, organizers of the event believe that SIGSAC will be a fertile breeding ground for future standouts. This advantage transfers well to other institutions because of the ongoing creation of similar interschool attack-defend competitions. Finally, each summer, our institution sends a select number of students to attend academic internships at a variety of information assurance related organizations. The most coveted slots being at the National Security Agency. Faculty members making these selections would frequently consult with SIGSAC faculty advisors to help determine those students that had a true passion for the field from their pool of otherwise qualified candidates.

2. Benefits

In addition to the specific benefits stated above, the chapter provided other more general benefits. Students became excited about the computing discipline. Chapter members came from all academic disciplines offered at our institution and gained a greater awareness of the importance of information assurance. Faculty members had a consolidated

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

pool of candidates available to advertise and promote new course offerings and research opportunities. Participation statistics helped identify motivated students and allowed for wise allocation of resources. Faculty members and students from many departments worked together on solutions across the spectrum of disciplines. Students and faculty gained valuable experience in leadership and built new relationships with external professionals and organizations in the field. Feedback from chapter members provided a viable and accessible mechanism to gauge student interests.

3. Risks

Chapter members behaved well and, to date, have not participated in any hacking incidents. While leaders attempted to mitigate risk and other issues, they did not consider several outcomes. They did not predict the rapid growth of the organization. It is difficult to build the infrastructure of a group that jumps from an idea to 450+ members in a short period of time. While leaders were aided by the ACM's online stockpile of student chapter resources, a group of this size also requires additional resources including faculty members, money, transportation, bookkeeping, and meeting facilities. The growth of the organization also caused concern among some leaders and a degree of unstated competition with other student professional organizations and clubs.

4. Activities Planning

Careful management of resources was always a key issue. The chapter had little or no direct funding. Leaders partnered with many existing activities to provide opportunities for chapter members at little or no cost. Leaders also took advantage of our institution's unique relationships and access to provide a varied program. We submit that other institutions can do the same by looking to their local community. For example, a local FBI field office or law firm could provide a briefing to students on cybercrime. Local companies involved with computer security as their main business could provide seminars or sponsor summer internships. The university's information technology department could provide similar types of experiences and knowledge.

VI. Future Work

In the future, leaders hope to maintain membership at the level of 10% of the student body while, at the same time, increasing the quality, depth and breadth of activities. This is an iterative process. By listening to student's desires, leaders can home in on activities that will maintain interest and still provide a positive perspective on information security.

Managing a group of this size requires solid long-term infrastructure. Attempts are ongoing to build a set of guides and place them on a campus network server to act as a repository of the group's institutional knowledge such as meeting checklists and lessons learned documents from previous event coordinators. A database backed chapter website is also critical to managing the membership information of a group this size. The website will also act as a historical archive of text and images of previous activities. Despite additional chapter leader positions, the current structure is taxed by the demands of such a large organization. Faculty advisors are considering a more distributed structure along the military model. This proposal would form a battalion with a battalion commander and staff of personnel, security, operations and logistics officers. Subordinate to the battalion commander would be company commanders and platoon leaders each responsible for a portion of the membership. Another proposal is one of incremental change by adding photographer/historian and webmaster positions. The six faculty advisors for the group all come from our institution's Electrical Engineering and Computer Science department. Finding interested faculty from some or all of the other academic departments to serve as advisors or liaisons would assist is gaining access to new opportunities and further promote interdisciplinary activities.

The diverse nature of the chapter is such that many subgroups rarely meet. Leaders hope to improve camaraderie and esprit de corps through increased opportunities for social interaction. In particular, the SIGSAC IWAR lab could serve as a 24-hour base of operations, where a member could stop by as time permits. An award system could recognize top performers. For example, a recruiting award could be used to spur future growth. A chapter logo contest and t-shirt sales are two other ways to build cohesion and provide a public face for the club among the student body. Topical movie nights and other social events are another avenue to be explored.

The SIGSAC IWAR lab, while initially successful, needs improvement in several areas. It is difficult to take students, albeit highly enthusiastic, and put them in front of a computer and expect them to properly configure it for defense or use it to examine an attack. A base level of knowledge is required for a satisfactory experience. One technique being considered is the construction of self-paced training packets that will provide hands on, but scripted, learning. Some other possible solutions include purchasing prepackaged network security training modules or DEFCON/Blackhat conference videos as well as recording in-house packages and sharing them from a centralized server. The IWAR lab could also be set up as a private wireless network and students could bring their own machines for controlled exercises.

The infrastructure of the lab is in constant flux and there is a need to retain some degree of control while allowing for easy reconfiguration. Maintaining a base image of the machines for easy re-imaging is one possible solution. There is also the potential to use the lab to conduct a proof of concept cyberdefense exercise with other non-military academic institutions. There is perhaps even the potential for this

activity to grow into something akin to the ACM programming contest.

While the initial community service activities were successful there is significant room for growth. A more formal program of outreach to local schools could be established. The information security awareness campaign could likewise be broadened. The chapter also offers opportunities for advanced individual research on information assurance topics. To date, there have been only a limited number of SIGSAC members who participated in independent research coursework. The short courses offered on physical security were successful, but there should be additional student prepared offerings.

In accordance with ACM policy, general membership in the chapter does not require ACM membership. Chapter leaders would like to continue to promote the membership benefits of such a professional organization as well as conduct more joint activities with the traditional ACM and IEEE student chapters and the larger national corps of SIGSAC members. Most of the efforts of the leaders have been devoted to developing and executing a high quality program. While this is very important, continued support from the institution is vital to the long-term success of the chapter. Increased visibility through national level publications, local news articles and the alumni magazine could help spread the word. Finally, the large membership of the group possesses a wide demographic background that would make an interesting population for the study of information assurance awareness and ethical behavior.

VII. Conclusions

There is a story to tell about our SIGSAC experience. We were able to tap into the enthusiasm of our student body and direct the interest into healthy areas that increased skills and awareness of the importance of information security. At our institution, virtually every student of every class has been introduced to SIGSAC and the basics of information security. We have more than five times as many SIGSAC members than we have computer science majors, including many from populations typically underrepresented in science and engineering. We believe that with creativity and enthusiasm other institutions can create similar groups that will greatly increase the breadth and depth of student, staff and faculty exposure to information assurance that will have a marked and positive impact on information security both now and into the future.

VIII. Acknowledgements

We would like to thank the hard working student leaders of the group, the Dean of the Academy, the leadership of the Department of Electrical Engineering and Computer Science, the faculty advisors who contributed their time and energies as well as all of the membership who made the group a success. We would also like to thank Dr. Melissa Dark of Purdue University, Dr. Wenke Lee and Dr. Ron Ferguson of the Georgia Institute of Technology and the anonymous reviewers for their candid and insightful feedback. Finally, we would like to thank Brett Meyers of Iowa State University and Jesse Vernon of Grinnell College for sharing their experiences as they create similar groups.

IX. References

[1] G. Conti, J. Hill, S. Lathrop, K. Alford and D. Ragsdale; "A Comprehensive Undergraduate Information Assurance Program;" Third World Conference on Information Security Education (WISE3); June 2003.

[2] Association for Computing Machinery Code of Ethics and Professional Conduct, http://www.acm.org /constitution/code.html, ACM accessed on 8 February 2004.

[3] Association for Computing Machinery at Colorado State University, http://www.cs.colostate.edu/~acm/benefits.html, accessed on 8 February 2004.

[4] Hintz, A.; “Promoting an Information Security Program via a Student Organization;” Colloquium for Information Systems Security Education; June 2002.

[5] Information Assurance Student Group, http://iasg.ece.iastate.edu/, accessed on 8 February 2004.

[6] Grinnell College Student Groups, http://www.grinnell.edu/student/groups/jnl/, accessed on 8 February 2004.

[7] Grinnell Hacking Club (LINK), http://www.lennalf.com/hack/, accessed on 8 February 2004.

[8] S. Lathrop, G. Conti and D. Ragsdale; "Information Warfare in the Trenches: Experiences from the Firing Line;" Third World Conference on Information Security Education (WISE3); June 2003.