Developing Faculty Expertise in Information Assurance through Case Studies and Hands-on Experiences

Xiaohong Yuan, Kenneth Williams, Huiming Yu
Department of Computer Science
North Carolina A&T State University
Greensboro, NC 27411
xhyuan|williams|cshmyu@ncat.edu

Bei-Tseng Chu, Audrey Rorer
Department of Software and Information Systems
University of North Carolina at Charlotte
9201 University City Blvd.
Charlotte, NC 28223
Billchu|arorrer@uncc.edu

Li Yang, Kathy Winters, Joseph Kizza
Department of Computer Science and Engineering,
The University of Tennessee at Chattanooga
Chattanooga, Tennessee, 37403
Li-Yang|Joseph-Kizza| Kathy-Winters@utc.edu

Abstract

Though many Information Assurance (IA) educators agree that hands-on exercises and case studies improve student learning, hands-on exercises and case studies are not widely adopted due to the time needed to develop them and integrate them into curriculum. Under the support of National Science Foundation (NSF) Scholarship for Service program, we implemented two faculty development workshops to disseminate effective hands-on exercises and case studies developed through multiple previous and ongoing grants, and to develop faculty expertise in IA. This paper reports our experience of holding the faculty summer workshops on teaching information assurance through case studies and hands-on experiences. The topics presented at the workshops are briefly described and the evaluation results of the workshops are discussed. The workshops provided a valuable opportunity for IA educators to connect with each other and form collaboration in teaching and research in IA.

1. Introduction

As our society becomes increasingly dependent on cyberspace, security and assurance of our computing infrastructure and cyberspace is vital to nearly all aspects of our lives and our social, economic and political system. The past decade has seen a large growth of computer security programs at colleges and universities. However, there are still many colleges and universities that either do not offer security education in their curriculum, or are in the beginning phase of providing security education.

Incorporating hands-on exercises and case studies is a proven effective pedagogy that can increase student interests and enhance their learning experience [1, 2, 3, 4]. Hands-on exercises and case studies allow students to apply their learning to the real world situations. Though many IA educators agree that hands-on exercises and case studies improve student learning, hands-on exercises and case studies are not widely adopted due to the time needed to develop them and integrate them into curriculum. Because IA is still a relatively new field, many instructors were not trained in IA and lack practical experience, and consequently they may not feel comfortable in using hands-on exercises or case studies in their classes.

Under the support of NSF Scholarship for Service program, we implemented two faculty development workshops to disseminate effective hands-on exercises and case studies developed through multiple previous and ongoing grants. This is through the collaboration of three universities that have long track records in IA education: North Carolina Agricultural and Technical State University (NC A&T), the University of North Carolina at Charlotte (UNC-Charlotte), and the University of Tennessee at Chattanooga (UTC). The overall goals of this project are to build faculty capacity in IA education and training, increase student interest and learning in IA and increase partnership between institutions in IA education.

We have successfully held the first week-long faculty summer workshop in May, 2012 at UTC and the second faculty summer workshop in May 2013 at NC A&T [5]. Nineteen faculty members attended the first workshop and twenty faculty members attended the second one. They are current IA faculty and are from institutions with a strong interest in, and with appropriate institutional commitment to introducing hands-on exercises and case studies during the academic year following each workshop. Ten participants are from minority institutes such as Historically Black Colleges and Universities (HBCUs) and Hispanic serving institutes. The diverse background of the attendees brought diversity to the project, which in turn built an open and diverse platform for interested instructors to innovate and share pedagogical approaches in IA. This workshop broadly spans the scope of the IA knowledge domain such as cryptography, access control, database security, cloud security, network security, security management, web security, secure coding, security ethics, and digital forensics.

This paper reports our experiences of holding these workshops. Section 2 introduces the hands-on labs and case studies presented at the workshop; Section 3 presents the findings from the evaluation of the workshops. Section 4 describes the improvement made to the 2013 workshop and section 5 concludes the paper.

2. Hands-on Labs and Case Studies Presented at the Workshop

This section introduces the various IA topics and the associated hands-on labs and case studies for teaching these topics presented at the workshop.

2.1 Cryptography

Cryptography is the basis for most of the other areas in IA education [8]. This session introduces hands-on labs and case studies on cryptography. The hands-on lab allows participants to experience cryptographic algorithms and mechanisms, especially increasing awareness of possible threats and attacks to various cryptographic techniques, such as linear attack to S-box, short-message attack to RSA cipher. Moreover, we help participants to incorporate case studies in cryptography in curriculum that simulates and captures real-world cryptographic applications. Case studies engage students in real-world settings, which inspire creativity of students and train them to adapt cryptography solutions to emerging areas, such as virtualization, healthcare, and mobile computing areas. The hands-on labs and case studies are available at: http://www.cryptolabs.tk/.

2.2 Access Control and Database Security

Access control is the collection of mechanism that enables an authority to control access to resources in information [8]. This session demonstrates how to apply theories of access control to laboratorial exercises using commercial database system. Three access control schemes are exercised: Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Mandatory Access Control (MAC). One of the DAC vulnerabilities lies in the fact that there is no control on flow of information. A Trojan horse, one of the attacks that exploit such vulnerabilities, will be implemented and evaluated. Implementing MAC will gracefully demonstrate to attendees how to mitigate the risk of Trojan horses by enforcing control on information flow. Labs in advanced topics including virtual private database, auditing, data masking will be covered because of their significance and popularity in industry practice. The labs are developed and exercised under Oracle 10g database systems, which were published in [18].

2.3 Cloud Security

Cloud computing is a technology that extends the realms of a computer network, creating an environment that offers scalability, better utilization of hardware, on-demand applications and storage, and lower costs over the long run. Cloud security is based on the notion that cloud users normally trust cloud service providers with their data. This means that they expect security, availability and performance. In addition to this delegated security, enterprise security officials must also create a secure connection to the cloud provider. The hands-on labs on cloud security for the workshop were based on initiating instances on the Amazon Cloud and securing the connections.

The first lab demonstrates how to create and launch an Amazon Cloud instance and then securely connect to the instance just launched. It demonstrates how to transfer files between the local machine and the just created and launched Amazon EC2 instance. The second lab demonstrates how to use MapReduce to process large data or parallel problems using big datasets based on large number of compute nodes or clusters.

2.4 Network Security

Concept visualization, motivated by the age-old adage “a picture speaks more than thousand words”, has been used in a variety of fields in computer science education, such as algorithms, computer networks, computer architecture and so on [12, 13, 15]. There has been growing evidence showing concept visualization systems are indeed effective when they engage learners in an active learning activity [11, 14]. Students will benefit from the interactive visualization as one of active learning approaches, that involve students in the classroom in activities that are meaningful and make them think about what they are doing [7]. Therefore, effective visualization tools are needed in IA education, which bear characteristics of active learning activities including interactive, simple to understand, short time frame, creative and motivational, sometimes collaborative, and relevant [17]. We introduced a series of interactive simulation tools developed at NC A&T to demonstrate network security and other security concepts in this session. The simulation tools are described below:

- **An animated simulation for packet sniffer.** This tool demonstrates visually how a packet sniffer works in a local area network environment, and how data packets are encapsulated and interpreted while going through the protocol stack.
- **A learning tool for Kerberos authentication architecture.** This tool consists of a series of four scenes that progressively demonstrate the ideas that underlie the design of Kerberos Authentication Architecture. Scenes include "Distributed Authentication," "Centralized Authentication," "Ticket-Granting Service," and "Kerberos System." Hacking scenarios are demonstrated for some scenes. Challenge questions are provided to quiz tool users to help them grasp the key points of the authentication architecture".
- **The visualization tool for wireless network attacks.** This tool includes a series of five demos that visualize the following attacks popular in wireless networks: Eavesdropping, Evil Twin, Man in the Middle, ARP Cache Poisoning, and ARP Request Replay. The tool also provides challenge questions to give the user a quiz on the animation he/she watched.
- **Interactive SYN Flood simulator**. This tool demonstrates the concepts of normal network traffic which displays how the TCP three way handshake works and how SYN flood occurs. It allows students to interact with the simulator and take challenge questions.
- **Firewall simulation game**. This interactive learning tool allows students to configure a virtual firewall to protect a virtual network in a game environment. Through this tool the students learn how to configure a firewall according to a given set of requirements, and become familiar with how to use commercial firewalls such as Cisco firewalls.
- **Stack overflow visualization**. This visualization tool demonstrates the impact of stack overflow, its cause and its defense. It simulates the line by line execution of a simple program showing the simplified contents of the program memory and stack. The user can provide input to the simulated program creating a stack overflow allowing them to see the effects.

These simulation tools were implemented using Macromedia Flash, and can be run through a browser. They can be accessed from [6].

Additionally, we introduced several hands-on lab exercises that demonstrate attack/defense methods. This session was highly hands-on with participants actively practicing these lab exercises.

- **Wireless network attacks lab.** These laboratory exercises demonstrate the following wireless network concepts or methods: wardriving, eavesdropping, WEP key cracking/decryption, Man in the Middle, ARP cache poisoning, MAC spoofing and defense techniques of some of the attacks.
- **Stack overflow lab**. These lab exercises provide students with hands on experience in stack overflows. Using a debugging tool, students examine the execution and memory addresses of a vulnerable program. They then craft an input file that will cause the victim program to execute arbitrary code.

2.5 Security Management

Security management is probably one of the most important topics that future employers may need expertise in, given that many security products (e.g., anti-virus software, firewall, intrusion detection and prevention systems) can deliver well-defined security mechanisms. However, security management is a topic typically overlooked in security courses in higher education institutions. This session introduces a series of case studies developed by NC A&T on areas of risk management, incident response planning, disaster recovery planning, security policy, and physical security. Each case study includes case learning objectives, case description and case discussion questions which were mapped into Bloom's Taxonomy. These case studies are available at [6].

2.6 Web Security

UNC Charlotte has developed a set of web applications for teaching web security. Although these applications were not designed for robustness and performance, they nevertheless have reasonably complete functionality. The applications include: online banking, online music store, micro-blog social network, and online health benefit management. All the applications are written in Java. These applications have commonly found vulnerabilities subject to attacks. The hands-on exercises include:

- **Vulnerability assessment.** Participants can use widely used attack methods to exploit vulnerabilities such as cross site scripting, SQL injection, forced browsing, privilege escalation, cross site request forgery, click jacking, session hijacking, and resetting passwords.

- **Secure programming.** Participants identify programming errors and practice secure design/coding. For example: proper input validation/output encoding using proven tools (e.g. OWASP ESAPI and AnitSammy), implement proper access control, proper error handling to avoid source code disclosure, proper session management, proper design of password management system, and explore emerging technologies such as Content Security Policy which hold the promise to prevent cross site scripting and click jacking.

2.7 Security Ethics

Ethics education is central to a rounded security education. This session facilitates participants to teach the ethical issues involved in information assurance using cases for relevancy. The basic concepts and principles are drawn from [9, 10]. This session began with a brief discussion of the ethical theories to assure everyone had the same foundation for analysis. The participants were divided into three groups and given the same current event article to read. Each group was given a different ethical theory from which to evaluate the validity of the actions taken. For example, for article 1, group 1 considered the point of view of Utilitarianism, group 2 considered the point of view of relativism, and group 3, the point of view of human nature. One person from each group was then asked to present the group findings to all participants. This exercise was repeated for a series of articles dealing with current event in information security and each time the group was asked to consider a new article from a different point of view.

2.8 Digital Forensics

Digital forensics is the application of computer investigation and analysis techniques which may include data recovery. This session introduced major forensics investigations of evidence gathering, acquisition, analysis, report writing and expert witness testimony through cases. These cases come with a working forensics investigator's toolbox consisting of ProDiscover (http://www.techpathways.com/ProDiscoverDFT.htm), FTK (http://accessdata.com/products/forensic-investigation/ftk), Encase (http://www.guidancesoftware.com/) and open source tools that cover a cross-section of platforms. In addition to these cases, other contemporary cases were discussed and worked on including cases like Cracking Encrypted CDs, Pivotal Palm Pilot Passwords, and Email Evidence Exposes, etc. [16].

3. Findings from Workshop Evaluation

The faculty summer workshop was evaluated through a pre-workshop faculty survey; a post-workshop faculty survey and faculty focus group study conducted at the end of workshop. The pre and post survey results and faculty focus group study results are described below. A recognized limitation of this project evaluation is in the sampling bias inherent in both faculty studies and student outcomes studies. Faculty and students display an inherent interest in IA topics in their election to participate in the IA Faculty Workshop, and in their enrollment in IA courses. However, the intended audience for the teaching tools is indeed faculty and students with interest in these topics. The overall goal is to provide sophisticated teaching tools that enhance and facilitate student learning, as well as faculty ability to deploy these tools. In the current project phase, we are able to report descriptive findings. An in depth comparative study of student learning outcomes is underway and is therefore beyond the scope of this paper.

The hypotheses for the project overall are as follows:

1) The hands-on faculty workshops are an effective means of enhancing faculty capacity to teach IA concepts;

2) The tools and resources provided by the hands-on faculty workshops are convenient and easily adaptable for faculty to incorporate into their IA curriculum; and

3) The tools and resources (i.e. hands-on labs and case studies) are effective IA teaching tools for undergraduate students.

Hypotheses 1 and 2 pertain to faculty participants in the workshops. The third hypothesis pertains to student learning outcomes, for which a full comparative study is currently underway. Summative results are provided in Section 3.1 and 3.2 describing faculty outcomes.

3.1 Faculty Pre and Post Survey Results

The pre and post surveys were designed to assess faculty self-reported knowledge gains and overall satisfaction with the workshop and materials. Faculty were asked to rate their level of understanding of security management, cryptography, network security, web security, and access control, on a five point Likert-type scale ranging from 0 (no knowledge) to 4 (expert level). Additionally, they were asked to rate their agreement levels on a similar five point Likert-type scale (1=strongly disagree through 5=strongly agree) on items pertaining to the development of case studies and hands-on lab activities as being useful for student learning, and on being difficult to develop. For the 2012 workshop, all 19 faculty workshop participants were invited to take the pre and post survey via Survey Monkey. A total of 18 faculty responded to the pre survey and 13 responded to the post survey. Given the small number of workshop participants, a non-parametric analysis, the Mann-Whitney U test was employed for assessing the mean score ranks between pre and post survey assessment. While no significant differences were found between pre and post assessment, all rankings increased, indicating knowledge gains and overall satisfaction with the workshop. These findings were corroborated in the focus group discussions. Table 1 below presents the pre and post survey assessment scores for the first workshop.

Given the interest and exposure to teaching IA topics of workshop attendees, the faculty pre-survey was omitted for the 2013 workshop. Of the 20 participants in the workshop, 18 responded to the post-survey. Findings were positive as evident in the mean ratings of knowledge levels, overall workshop satisfaction, and plans to use case studies and hands-on labs. Mean ratings of post-survey responses from 2013 are presented in Table 2.

Table 1. 2012 Faculty IA Workshop Pre and Post –Survey Responses

Items: Please rate your knowledge in the following areas:	Mean		Standard Deviation	
	Pre	Post	Pre	Post
Security Management	2.14	2.63	1.09	0.80
Cryptography	2.64	2.90	0.84	0.53
Network Security	2.57	3.18	1.01	0.60
Web Security	2.42	2.81	0.85	0.60
Access Control	2.42	2.90	0.93	0.53
Please indicate your agreement with the following:				
Case studies and hands-on labs are hard to develop	3.78	4.09	0.80	0.70
Case studies and hands-on labs are a useful way to teach IA	4.57	4.64	1.08	0.92

Table 2. 2013 Faculty IA Workshop Post-Survey Responses

Items: Please rate your knowledge in the following areas:	Mean	Std. Deviation
Security Management	3.56	0.62
Cryptography	3.93	0.68
Network Security	4.18	0.65
Web Security	3.75	0.85
Access Control	3.87	0.61
Please indicate your agreement with the following:		
Case studies and hands-on labs are hard to develop	4.12	0.88
Case studies and hands-on labs are a useful way to teach IA	4.81	0.40

Following both workshops, faculty indicated the opinion that developing case studies and hands-on lab activities was more difficult prior to the workshop. This is likely a result of having had a deeper exposure to the teaching techniques. The belief that these are useful teaching methods increased as a result of the workshop, therefore indicating that the faculty participants believe these tools are worthwhile.

Overall, faculty unanimously agreed that they were satisfied with the workshop. All indicated plans to implement the lab activities taught in the workshop in their future courses; all but one respondent indicated plans to implement the case studies within their courses. Several faculty indicated that the opportunity to meet others who are engaged in teaching IA topics was useful. A few helpful suggestions were noted following the 2012 workshop: to facilitate peer networking, increase brainstorming and time to 'play' with the tools. The majority indicated desiring technique documentation, and all workshop materials provided to them via disk or some other mechanism. Revisions to the materials, content and delivery of the 2013 workshop were made to address these formative findings, presented in section 4.

3.2 Faculty Focus Group Study Results

A total of three focus groups were conducted during the IA Workshop in 2012 and two focus groups during the 2013 workshop. A total of 36 faculty participated out of 39 total participants in the workshop. Participation in the focus groups was voluntary. All participants were informed of confidentiality procedures prior to the start of each focus group.

An overview of themes from each question asked is outlined in Table 3.

Table 3. Faculty Focus Group Study Results

1. Background of the faculty participants, how they became interested in teaching:
• Most faculty have taught IA courses and topics for at least 5 years, a few were new to IA and plan to teach in the area within the next year. • All reported that they find IA exciting, interesting and the most dynamic component within computer science/technology.
2. Challenges in teaching IA:
• All reported bureaucratic and policy barriers to teaching IA at their institutions, noting- o Administration prohibiting use of labs for hacking, for fear of breach in campus security overall. o Lacking financial support in purchase of proprietary software and tools. • Student challenges noted were: lack of interest in and understanding of theoretical & policy components; faculty reported boredom with these topics. "Students want to *do* something." • Managing student expectations- "it's not what they think it is." • Unappealing nomenclature (Information Assurance) does not attract students.
3. Effective ways to increase student participation
• All agreed that use of hands-on activities, case studies and labs would engage their students. "I feel empowered that I can do more in my classes." • All noted a dearth of IA of teaching tools, which prompted them to participate in the workshop.
4. Participation in prior professional development for IA teaching
• Only five faculty indicated participating in IA workshops that were specifically about teaching techniques, and both indicated it was several years ago. • Motivation for participation in the workshop was: o Needing fresh methods/tools/techniques to teach. o Specifically seeking hands on activities and lab materials.
5. Tools from this workshop they plan to use were:
• Everyone reported intention to use Virtual Machines (VMs) because it solves the bureaucratic challenges at their institutions that are noted above. • Security First, Firewall Game, Cryptool, Interactive Simulation/Visualization tools. • Case studies for class discussion. • Buffer Overflow modules, secure coding module

6. Tools/techniques they are unlikely to use and why:
• Some mentioned the labs based on Oracle and Amazon Cloud since they are expensive to purchase. • Some mentioned Wireless Network Attack labs because they are difficult to understand.
7. Collaborations that have been made possible:
• They unanimously agreed that the workshop has been useful in connecting them with one another. "I know I can reach out to anyone in this group." • They desire a group site for discussion as well as a document site for materials.

In response to the overall feedback from faculty participants about desiring ways to continue networking, sharing ideas and to obtain workshop materials and documentation, two tools have been deployed. A Google discussion group was created at the close of the 2012 workshop as a mechanism for the participants to remain connected, and to have a vehicle for discussion threads and resource sharing. A shared documents folder has also been established to provide all workshop materials as an accessible online resource. Following the 2013 workshop, plans are to establish a Linked In Group.

3.3 Evaluating the Effectiveness of Workshop Materials on Student Learning

Faculty who were teaching courses in security management, cryptography, network security, web security and access control during the spring 2012 and spring 2013 terms prior to their workshop participation were asked to invite their students to participate in a survey of interest, confidence and knowledge of those IA topics. This survey includes a pre-survey at the beginning of the Spring 2012 term and a post-survey at the end of the Spring 2012 term designed to measure learning outcomes in the respective content areas of IA. This data will be utilized as baseline data for comparative purposes, i.e. the same faculty courses will participate in the pre-post- survey to see if student interest, confidence and knowledge gains are improved following the adoption of the cases and hands-on labs presented at the workshop.

Currently we are conducting follow-up assessment on the adoption of the tools by the workshop participants in the courses they teach after the workshop. The same student pre- and post-survey that was conducted before their participation of the summer workshop will be conducted again in their respective IA courses. This data will be compared with the baseline data to see if student interest, confidence and knowledge gains are improved following using the workshop tools in teaching IA topics. Additionally, we are following up with faculty who were invited and/or registered for the workshop but did not attend, to explore their teaching methods and student outcomes as another source of like comparison groups.

4. Improvement Made to the 2013 Faculty Workshop

Revisions to the materials, content and delivery of the 2013 faculty workshop were made to address the formative findings of the 2012 faculty workshop. These revisions are listed below:

- The schedule of the 2013 workshop was revised to allow enough time for faculty participants to develop expertise in IA hands-on labs.
- We started the 2013 workshop with an orientation so that everyone can introduce themselves and their background - this helped workshop participants to get to know each other, enabled collaboration and future follow up contact.
- We formed small working groups to brainstorm necessary measures and directions that will improve transferability of hands-on labs, and student learning in IA.

5. Conclusion

This paper reports our experience of holding summer workshops on teaching information assurance through case studies and hands-on experiences. The topics presented at the workshop were briefly described and the evaluation results of the workshop were discussed. Overall, faculty unanimously agreed that they were satisfied with the workshop and felt that the case studies and hands-on labs presented at the workshop are worthwhile. They all plan to adopt most of the case studies and/or hands-on labs in their courses. To evaluate the effectiveness of the tools in student learning, we are conducting on-going follow-up assessment on the adoption of the tools by the workshop participants in the courses they teach after the workshop and measuring student learning outcomes comparatively.

We presented the faculty perspective which demonstrates the value of cross-institutional collaborations regarding teaching practice. Faculty workshop participants reported that conference attendance is focused on research conferences, rather than those with an educational focus. These workshops have provided the faculty with innovative teaching tools and resources, reduced the development time for new teaching approaches, and connected faculty with a group of peers who engage in IA topics, and can pull a collective expertise. This workshop has been valuable in connecting them with one another and form collaboration in teaching and research.

Our experience with the workshop shows that in order for a case study or hands-on lab to be widely adopted by instructors of IA, it is very important to provide good documentation such as step-by-step instructions, exercise questions, tests, solutions etc., as well as provide peer technical support. A platform and community that support sharing of IA hands-on labs/cases and achieving the effectiveness and transferability of these labs/cases are needed in the IA education community.

6. Acknowledgement

This work is partially supported by NSF under grant DUE-1129413, 1129444, and 1129355. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

7. References

[1] Brustoloni, J. C. “Laboratory experiments for network security instruction,” *ACM Journal on Educational Resources in Computing*, Vol. 6, No. 4, 2006.

[2] Du, W and Wang, R. SEED: A Suite of Instructional Laboratories for Computer Security Education (Extended Version). In *The ACM Journal on Educational Resources in Computing (JERIC)*, Volume 8, Issue 1, March 2008.

[3] Yuan, X., Jiang, K., Murthy, S., Jones, J. and Yu, H., “Teaching security management with case studies: experiences and evaluation,” *Journal on Education, Informatics and Cybernetics (JEIC)*, accepted, 2011.

[4] Penn State University Teaching and Learning Technology, Using cases in teaching, available at: http://tlt.its.psu.edu/suggestions/cases/index.html, retrieved, February 8, 2011.

[5] Hands-on Information Assurance: Teaching Information Assurance through Case Studies and Hands-on Experiences. Retrieved on January 22, 2013 from https://teaching-ia.appspot.com/workshop/about

[6] Teaching Information Security Using Visualization Tools, Case Studies, and Hands-on Exercises. Accessed on January 22, 2013 from http://williams.comp.ncat.edu/IA_visualization_labs/

[7] Bonwell, C., and Eison. J., “Active Learning: Creating Excitement in the Classroom,” *ASHE-ERIC Higher Education Report* 1, 1991.

[8] Cooper, S., Perez, L., and Oldfield, B., Towards Information Assurance Curricular Guidelines, in *Proceedings of the 15th Annual Conference on Innovation and Technology in Computer Science Education (ITiCSE)*, Turkey, June, 2010.

[9] Kizza, J. M., *Computer Network Security and CyberEthics*, Second Edition. McFarland & Company, 2006.

[10] Kizza, J. M. *Ethical and Social Issues in the Information Age*. Third Edition, Springer-Verlag, New York, 2007.

[11] Grissom, S. et al. 2003. Algorithm visualization in CS education: comparing levels of student engagement, in *Proceedings of ACM 2003 Symposium on Software Visualization*, 87-93, 2003.

[12] GVU, Algorithm animation. Available at http://www.cc.gatech.edu/gvu/softviz/algoanim/,2002.

[13] Holliday, M. A. 2003. Animation of computer networking concepts, *ACM Journal of Educational Resources in Computing*, Vol. 3, No. 2, Article 2.

[14] Naps, T. L. et al. 2003a. Exploring the role of visualization and engagement in computer science education, *ACM SIGCSE Bulletin*, Vol. 35, Issue 2, 131-152, 2003.

[15] Null, L. and Rao, K., 2005. CAMERA: Introducing memory concepts via visualization, In *Proceedings of the 36th SIGCSE Technical Symposium*, St. Louis, Missouri, Feburary 23-27, 2005, 96-100.

[16] Palmer, A., The Top Ten Most Unusual Computer Forensics Cases, 2008. http://www.krollontrack.co.uk/publications/UK_V5_AP_CF.pdf, retrieved, Jan. 2011.

[17] Schweitzer, D., Brown, W., “Interactive Visualization for the Active Learning Classroom,” In *Proceedings of the ACM Technical Symposium on Computer Science Education (SIGCSE)*, March 7-10, 2007.

[18] Yang, L., Teaching Database Security and Auditing, *Proceedings of the 40th ACM Technical Symposium on Computer Science Education (SIGCSE)*, Chattanooga TN, March, 2009.