Journal of Information Systems Education

Volume 28
Issue 1
November 2017

Faculty Workshops for Teaching Information Assurance through Hands-On Exercises and Case Studies

Xiaohong Yuan, Kenneth Williams, Huiming Yu, Audrey Rorrer, Bei-Tseng Chu, Li Yang, Kathy Winters, and Joseph Kizza

Recommended Citation: Yuan, X., Williams, K., Yu, H., Rorrer, A., Chu, B.-T., Yang, L., Winters, K., & Kizza, J. (2017). Faculty Workshops for Teaching Information Assurance through Hands-On Exercises and Case Studies. *Journal of Information Systems Education,* 28(1), 11-20.

Article Link: http://jise.org/Volume28/n1/JISEv28n1p11.html

Initial Submission: 29 January 2016
Accepted: 10 April 2017
Published: 7 November 2017

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Faculty Workshops for Teaching Information Assurance through Hands-On Exercises and Case Studies

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

Audrey Rorrer
Diversity in Technology Institute
University of North Carolina – Charlotte
Charlotte, NC 28223, USA
Audrey.Rorrer@uncc.edu

Bei-Tseng Chu
Software and Information Systems
University of North Carolina – Charlotte
Charlotte, NC 28223, USA
billchu@uncc.edu

Li Yang
Kathy Winters
Joseph Kizza
Department of Computer Science and Engineering
University of Tennessee – Chattanooga
Chattanooga, TN 37403, USA
Li-Yang@utc.edu, Kathy-Winters@utc.edu, Joseph-Kizza@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 curricula. Under the support of the National Science Foundation (NSF) Scholarship for Service program, we organized two faculty development workshops to disseminate effective hands-on exercises and case studies developed through multiple previous and ongoing grants. To develop faculty expertise in IA, the workshop covered a wide range of IA topics. This paper describes the hands-on exercises and case studies we disseminated through the workshops and reports our experiences of holding the faculty summer workshops. The evaluation results show that workshop participants demonstrated high levels of satisfaction with knowledge and skills gained in both the 2012 and 2013 workshops. Workshop participants also reported use of hands-on lab and case study materials in our follow-up survey and interviews. The workshops provided a valuable opportunity for IA educators to communicate and form collaborations in teaching and research in IA.

Keywords: Faculty development, Experiential learning & education, Case study, Information assurance & security

1. INTRODUCTION

As cyber security becomes a critical area that impacts our society and daily life, many universities and colleges have developed or are developing cyber security programs. This requires building the capacity of faculty in universities and colleges to effectively teach cyber security curricula. One approach is through faculty development workshops for developing expertise in cyber security education.

Numerous authors have developed hands-on labs and case studies to teach cyber security, and they have shown them to be effective pedagogy (Brustoloni, 2006; Du and Wang, 2008; Sanders, 2003; Spears and Parrish, 2013; Yuan et al., 2014). The authors implemented two, week-long faculty development workshops for teaching information assurance (IA) using hands-on labs and case studies with the support from the National Science Foundation (NSF). These hands-on labs and case studies were developed through multiple previous grants funded by NSF. The objectives of the workshops were to build faculty capacity in IA education and training, increase student interest and learning in IA, and increase partnerships between institutions in IA education. The first week-long faculty summer workshop was in May 2012, at the University of Tennessee – Chattanooga (UTC). The second faculty summer workshop was in May 2013, at North Carolina Agricultural and Technical State University (NC A&T). Nineteen faculty members attended the first workshop, and twenty faculty members attended the second one. The faculty participants were from diverse universities including minority institutes such as Historically Black Colleges and Universities (HBCUs) and Hispanic Serving Institutions (HSIs). The topics presented at these workshops broadly span the scope of the IA knowledge domain including cryptography, access control, database security, cloud security, network security, security management, web security, security ethics, and digital forensics.

Hands-on workshops have been used to develop faculty capacity in technology fields (Jackson et al., 2014; Taclehaimanot and Lamb, 2005; Wagner and Phillips, 2006). Wagner and Phillips describe a computer security training workshop they implemented to help faculty members develop their own courses and laboratory exercises on computer security. This workshop was six hours long and introduced topics such as foot printing and packet sniffing, port scanning, password policy and cracking, vulnerability assessment, system hardening, intrusion detection, and cyberwar exercises. The workshop series we held were the collaborative efforts of three universities which acquired NSF funding to develop hands-on labs and case studies on various topics of cyber security. Therefore, the hands-on labs and case studies presented cover a much wider area of topics. This paper describes the hands-on labs and case studies presented at our workshops and our experiences with building faculty capacity in cyber security education through workshops. The objective is to help other cyber security educators be aware of such resources and adopt and adapt such resources into their teaching.

The rest of the paper is organized as follows. Section 2 introduces the hands-on exercises and case studies presented at the workshops. Section 3 presents the evaluation of the effectiveness of the workshops on building faculty capacity in IA. Section 4 concludes the paper.

2. HANDS-ON LABS AND CASE STUDIES PRESENTED AT THE WORKSHOPS

This section introduces the various IA topics and the associated hands-on labs and case studies for teaching these topics presented at the workshop. These topics were selected based on the expertise of the authors and the hands-on labs and case studies developed by the authors. These hands-on labs and case studies can be incorporated into junior/senior level undergraduate courses such as Introduction to Information Assurance/Cyber Security, Network Security, Cryptography, Web Security, Security Management, etc. The prerequisites for such courses are CS1 and CS2 courses.

2.1 Cryptography

This session introduced hands-on exercises on cryptographic algorithms and mechanisms. It also introduced possible threats and attacks to various cryptographic techniques, such as linear attack to S-box and short-message attack to RSA cipher. Hands-on labs contain two parts with one using Cryptool and the other using programming languages. Cryptool labs include the topics of 1) encryption using binary/byte addition, 2) encryption using binary Exclusive-OR (XOR), 3) Triple DES with CBC mode and Weak DES keys, 4) RSA Encryption and Factorization Attacks, 5) attack on RSA encryption with short RSA modulus, 6) hash generation and sensitivity of hash functions to plaintext modifications, 7) Digital Signature Visualization, 8) RSA Signature, and 9) attack on Digital Signature/Hash Collision. Programming labs explore various attacks to encryption ciphers such as frequency analysis, short message attacks to RSA, timing attacks to RSA, tampering hash function, etc. More resources are available at: http://web2.utc.edu/~djy471/cryptography/crypto.htm.

2.2 Access Control and Database Security

Topics introduced in this session included labs on Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Mandatory Access Control (MAC). DAC policies control access based on the identity of the requestor and on access rules stating what requestors are (or are not) allowed. DAC policies of a database system can be implemented by an access matrix model which regulates the privileges that a subject can have on an object. In order to develop an access control model, we identify objects to be protected, subjects that execute activities and request access to objects, and actions that can be executed on the objects. An object can be a table, a view, a procedure, or any other database object. A subject can be a user, a role, a privilege, or a module. MAC policies control access based on mandated regulations determined by a central authority. RBAC policies control access depending on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles. One lab demonstrated how to use a Trojan horse to exploit the vulnerability of DAC (i.e., there is no control on the flow of information). To complement this lab, another lab demonstrated how to implement MAC to mitigate the risk of Trojan horses by enforcing control on information flow. Labs in advanced topics including virtual

private database, auditing, and data masking were also covered due to their significance and popularity in industry practice (Yang, 2009). More resources are available at: http://teaching-ia.appspot.com/labs.

2.3 Cloud Security

Understanding players and their roles, application, or data in play helps to understand cloud security. Cloud providers, customers who are the data owner and who seek cloud services from the cloud provider, and users who may or may not be the owner of the data stored in the cloud are the main players in cloud security. We discuss the access control processes for three of the top cloud providers to fully understand the roles and responsibilities assigned to each player: 1) Amazon Web Services (AWS), 2) Microsoft Windows Azure, and 3) Rackspace. Amazon Web Services (AWS) EC2 uses Amazon Identity and Access Management (IAM) which allows the account owner to create multiple accounts for other authorized users on a single Amazon account. Each user is then assigned permissions on the main account, accessible via a userid and password based on the user's role and responsibility in the customer's company. Based on the traditional access control, fine-grained security can be attained for all service users. Microsoft Azure uses a home grown Azure Platform AppFabric Access Control Service (ACS) to manage user access security. Key Features of ACS include: integration with Windows Identity Foundation (WIF) and tooling; out-of-the-box support for popular web identity providers; out-of-the-box support for Active Directory Federation Services 2.0; support for OAuth 2.0 (draft 13), WS-Trust, and WS-Federation protocols; support for the SAML 1.1, SAML 2.0, and Simple Web Token (SWT) token formats; integrated and customizable Home Realm Discovery that allows users to choose their identity provider; and a Web Portal that allows administrative access to ACS configuration. Rackspace uses client authentication called Cloud Authentication Service, also known as Auth, which allows each client needing authentication to obtain an authentication token and a list of regional service endpoints to the various services available in the cloud. Users must authenticate with their credentials, but once authenticated they can create/delete containers and objects within that account.

We introduce a hands-on lab based on Amazon Elastic Compute Cloud (Amazon EC2). Amazon EC2 is a web service that provides computing capacity in the cloud and allows user to run applications on Amazon's computing environment with inexpensive cost (Amazon EC2 – Virtual Server Hosting, 2016). This lab demonstrated how to create and launch an Amazon EC2 Cloud instance, establish a secure connection to the instance, and transfer files between the local machine and the instance. More resources are available at: http://teaching-ia.appspot.com/labs.

2.4 Network Security

Labs used to demonstrate network security and other security concepts were introduced in a series of interactive simulation tools developed at NC A&T. These simulation tools are described below. More resources are available at http://williams.comp.ncat.edu/IA_visualization_labs/.

- **An animated simulation for packet sniffer.** This tool demonstrates visually how a packet sniffer works in a local area network (LAN) environment and how data packets are encapsulated and interpreted while going through protocol stacks (Yuan et al., 2010b). The local area network is depicted as two subnets connected with a router. The two subnets have star and bus topologies, respectively. The visualization includes five parts. The first four parts show how a data packet moves from the source to destination computer following the direct path, the real path with subnets, with the network interface card being configured in promiscuous mode, and with a packet sniffer. The fifth part of the demo displays a TCP/IP protocol stack and animates the encapsulation and de-encapsulation process.
- **A learning tool for Kerberos authentication architecture.** This tool visualizes a series of four scenes that progressively demonstrate the ideas that underlie the design of Kerberos Authentication Architecture (Yuan et al., 2010b). The four scenes are:

    1) *Distributed Authentication*. This scene demonstrates the authentication mechanism in which each service server (e.g., email server, file server) has a user password database and verifies the user password to authenticate the user. The user's ID and password are sent in plaintext.
    2) *Centralized Authentication*. This scene demonstrates the authentication mechanism in which an Authentication Server (AS) is added which has a centralized password database. When the user requests a service, AS verifies the user credentials, creates a service server ticket, and sends it to the user. The user then sends this service server ticket along with user ID to the service server. The service server verifies user ID and sends the requested information to the user if the user is verified.
    3) *Ticket-Granting Service*. This scene demonstrates the authentication mechanism in a Ticket-Granting Service (TGS) where the client first requests a ticket-granting ticket from the Authentication Server, then requests a service ticket from Ticket-Granting Server. Finally, the client uses the service ticket to request service from the server.
    4) *Kerberos System*. The Kerberos protocol authenticates users to servers and servers to users. It counters a replay attack using session keys and authenticators.

Hacking scenarios are also demonstrated for some of the scenes. Challenge questions are provided to quiz users to help them grasp 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:

    1) *Eavesdropping*. This demo visualizes how a hacker eavesdrops on the communication between two wireless nodes. The attacker configures his/her network interface card (NIC) into promiscuous mode.
    2) *Evil Twin*. The demo visualizes the scenario that an attacker creates an evil twin or rogue access point (a wireless access point that masquerades as a legitimate one), and the user is connected to the evil twin.
    3) *Man in the Middle*. This demo visualizes the scenario that the attacker sets up a rogue access point which serves as the Man in the Middle between the user and the legitimate access point.
    4) *ARP Cache Poisoning*. This demo visualizes how the attacker causes incorrect IP/MAC address mapping to be added to a computer's ARP (Address Resolution Protocol) cache and then acts as a Man in the Middle.
    5) *ARP Request Replay*. This demo visualizes the scenario that the attacker conducts an ARP request replay attack to collect initialization vectors for cracking the WEP encryption key.

The tool also provides challenge questions to give the user a quiz on the animation he/she watched.

- **Interactive SYN flood simulator**. This simulator demonstrates the concepts of normal network traffic, how the TCP three way handshake works, and how SYN flood occurs. It allows students to interact with the simulator and answer 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. Each student takes the role of a network administrator who must configure the firewall to protect their network. Students may take actions against the networks of other students. The actions may be benign, such as reading from their virtual network's web server, or a malicious attack. If the student's firewall is not properly configured, they lose a point and the attacker gains a point. The scoring and game atmosphere motivates the students to do their best. Through the use of this tool, students learn how to configure a firewall according to a given set of requirements and how to use commercial firewalls such as Cisco firewalls.
- **Stack overflow visualization**. Using this set of tools, students experience attacks from stack overflow, its cause, and its defense. It simulates the line-by-line execution of a simple program demonstrating content of the program memory and stack. The user can provide input to the simulated program creating a stack overflow and maliciously change the program behavior. Different overflow attacks (such as changing the value of a variable or inserting code) and their defense are demonstrated and visualized.

Additionally, we introduced several hands-on lab exercises that demonstrate attack/defense methods.

- **Wireless network attack exercises.** This set of laboratory exercises demonstrate the following wireless network concepts or methods: war driving, 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**. In this lab, students use the built-in debugging tool in Microsoft Visual Studio to examine the execution and memory addresses of a vulnerable program. Students can then craft an input file that will cause the victim program to execute arbitrary code. Students follow step-by-step instructions to change the return address on the stack to jump to new machine language inserted from the input file. A virtual machine is used to provide a Windows XP environment that is easier to attack.

2.5 Security Management

This session introduced a series of case studies on areas of risk management, incident response planning, disaster recovery planning, security policy, and physical security. Each case study includes case learning objectives, the case description, and case discussion questions which are mapped to Bloom's Taxonomy (Yuan et al., 2010a). The case studies are available at http://williams.comp.ncat.edu/IA_visualization_labs/.

2.6 Web Security

This session introduced hands-on labs on vulnerability assessment for web applications. Participants used various attack methods to exploit vulnerabilities in web applications such as cross site scripting, SQL injection, forced browsing, privilege escalation, cross site request forgery, clickjacking, session hijacking, and resetting passwords (Chu et al., 2009).

2.7 Security Ethics

This session introduced the ethical theories (Kizza, 2006, 2007), and specific ethical security scenarios were given followed by group discussion to evaluate the validity of the actions taken in a current event using a particular ethical theory. Each scenario was a current event and demonstrated how students could learn to evaluate current events for their ethical and security ramifications.

2.8 Digital Forensics

This session introduced major forensics investigations of evidence gathering, acquisition, analysis, report writing, and expert witness testimony through cases. These cases came with a working forensics investigator's toolbox consisting of ProDiscover (Prodiscover Basic, 2016), FTK (Forensic Toolkit, 2016), EnCase (EnCase, 2016), and open source tools that cover a cross-section of platforms. Other contemporary cases such as Cracking Encrypted CDs, Pivotal Palm Pilot Passwords, and Email Evidence Exposes, etc. (Palmer, 2005) were also discussed.

A table listing the topics, hands-on labs, and teaching cases presented at the workshops, as well as the websites hosting the materials or references where more information can be found about the materials, is included in the Appendix.

3. EVALUATING THE EFFECTIVENESS OF THE WORKSHOPS

The hypotheses for the evaluation of the workshops pertaining to faculty were: 1) faculty workshops are an effective means of enhancing faculty capacity to teach IA concepts and an effective means of building partnerships and collaborations across institutions and 2) the tools and resources provided by the faculty workshops are convenient and easily adaptable for faculty to incorporate into their IA curricula. These hypotheses were examined in multiple ways. Faculty workshop participants were invited to participate in pre-workshop and post-workshop surveys, including a longitudinal follow up survey of teaching method deployment, and in focus groups held on the last day of the workshops. The assessment results are presented below.

3.1 Faculty Pre- and Post-Survey Results

For the 2012 workshop, pre- and post-surveys were conducted to assess faculty self-reported knowledge gains and overall satisfaction with the workshop and materials presented at the workshop. Faculty were asked to rate their level of understanding in different areas of IA on a five point Likert-type scale ranging from 1 (no knowledge) to 5 (expert level). They were asked to rate their agreement levels on a similar five point Likert-type scale ranging from 1 (strongly disagree) to 5 (strongly agree) on items pertaining to the development of hands-on exercises and case studies as being useful for student learning and on being difficult to develop. Of the 19 faculty workshop participants from the 2012 workshop, 18 faculty responded to the pre-survey and 13 responded to the post-survey. Table 1 presents the pre- and post-survey assessment scores for the 2012 workshop.

The Mann-Whitney U test was employed for assessing the mean ranks between pre- and post-survey assessment. It was found that all rankings increased from pre- to post-survey, though the difference was not statistically significant (with a 5% significance level). This indicated knowledge gains of the workshop participants, increased appreciation of the usefulness of hands-on labs and cases studies in teaching IA, and difficulties in developing them. The increased appreciation of the difficulties involved in developing hands-on labs and case studies was likely a result of having had a deeper exposure to the teaching techniques through the workshop. The increased appreciation of the usefulness of hands-on labs and case studies in teaching IA indicated that the faculty participants believe the tools presented at the workshop were worthwhile.

Please rate your knowledge in the following areas	Mean		Standard Deviation	
	Pre	Post	Pre	Post
Security Management	2.68	3.29	1.36	1.00
Cryptography	3.30	3.63	1.05	0.66
Network Security	3.21	3.98	1.26	0.75
Web Security	3.03	3.51	1.06	0.75
Access Control	3.03	3.63	1.16	0.66
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 1. 2012 Faculty IA Workshop Pre- and Post-Survey Responses

3.2 Faculty Focus Group Study Results

Three focus groups were interviewed during the 2012 workshop, and two focus groups were interviewed during the 2013 workshop. Out of 39 total workshop participants, 36 faculty participated in the focus groups. Overall, faculty participants unanimously agreed that they were satisfied with the workshops. Aspects of the workshops that the participants were satisfied with include: 1) the workshops provided the participants with innovative teaching tools and resources, 2) the workshops reduced the development time for new teaching approaches, and 3) the workshops connected faculty with a group of peers who engage in IA research and education. All indicated plans to implement the hands-on lab activities and case studies they learned in the workshop in their future courses.

3.3 Faculty Participant Follow-Up

A follow-up survey was conducted in the fall of 2013 with all faculty participants. Twenty two of the 38 participants responded, indicating a strong response rate of over half (58%). All but three reported using the case studies and hands-on activities as teaching tools. Among the few who did not use these tools, they indicated that they were not teaching IA courses or they had campus barriers preventing the deployment of certain lab tools.

Faculty follow-up surveys indicated that faculty participants were in fact implementing the tools presented in the workshops. Most faculty participants reported that the teaching methods were effective. The following are some of the comments made by the faculty participants:

- This material enhanced the students' learning a lot because it gave them real world situations. It made them apply what was in the book to the situation in the case study.

- I think that the materials enhanced the learning outcomes to a great degree. For the past two years, I have conducted a survey of learning outcomes, and the students' comprehension statistically increased over the results from the same survey given to the same class in 2011, before I attended the workshop.
- Students were really engaged.
- My students really enjoyed doing [the case studies].

3.4 Comparison Faculty Group

There were an additional 23 applicants who did not attend the workshops due to space limitations. It is assumed that this group of faculty share similar interests and experiences in IA teaching to the group who actually did participate and that they are as likely to seek out and adopt new teaching practices. The same workshop follow-up survey was distributed to workshop participants and non-participants to determine if workshop attendees reported more usage of hands-on exercises and case studies than the faculty who could not participate in the workshop. A small response rate of 35% was obtained for the comparison group of faculty non-participants, therefore survey findings may not apply to the entire group (n=23). However, it is notable to report the differences in perceptions of teaching and use of teaching methodologies between the workshop attendees and non-attendees. Non-participant faculty reported less knowledge of IA concepts than those who did participate (Table 2). They also reported a belief that using hands-on exercises and case study methods was difficult (86%) more often than participants (81%). Faculty who applied to but did not attend the workshop also reported using hands-on exercises and case studies less frequently (26%) than the group of faculty who participated in the IA Workshops (35%).

IA Topical Knowledge	Post-Workshop Faculty	Non-Participating Faculty
Security Management	2.25	2.15
Cryptography	3.4	2.85
Network Security	2.9	2.85
Web Security	2.4	1.45
Access Control	3.25	2.15

Table 2. Faculty Self-Rated Knowledge of IA Topics at the Working Knowledge Level

In summary, the assessment results described in the above sections on evaluating the effectiveness of workshops on building faculty capacity highlight the following findings:

- Faculty workshop participants reported high levels of satisfaction with the content and tools and the knowledge gains in the 2012 and 2013 workshops.
- Faculty reported adoption of case study materials and tools presented at the workshops in subsequently taught courses and ease of use.

These indicate the goals of the workshops pertaining to faculty were met.

4. CONCLUSION

This paper reports our experience of holding two faculty summer workshops on teaching information assurance through hands-on exercises and case studies. The topics presented at the workshop span a wide range of IA topics, including cryptography, access control, database security, cloud security, network security, security management, web security, security ethics, and digital forensics. The effectiveness of the workshops on building faculty capacity was evaluated. Compelling evidence from key indicators suggest the workshop goals were met. Faculty capacity for teaching IA concepts was greatly enhanced, as demonstrated by their survey responses, focus group conversations, and a comparison of similar faculty who did not participate in the workshops. Overall, faculty participants were satisfied with the workshops and believed that the hands-on exercises and case studies showcased at the workshop are useful teaching tools. Adoption of the tools was widespread.

We presented the faculty perspective which demonstrates the value of cross-institutional collaborations regarding teaching practice. Faculty workshop participants reported that conference attendance focused on research conferences, rather than those with an educational focus. These workshops have provided the faculty participants 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. These workshops have been valuable in connecting them with one another and forming collaboration in teaching and research.

Our experience with the workshop shows that in order for hands-on exercises and case studies to be widely adopted by instructors of IA, it is important to provide good documentation such as step-by-step instructions, exercise questions, tests, solutions, etc., as well as provide peer technical support. Future work could include developing a platform and community that supports sharing and effective adoption of IA hands-on exercises and case studies. Future work also includes evaluating the effectiveness of IA hands-on exercises and case studies using educational research methods; for example, using control group and experimental group comparisons.

6. ACKNOWLEDGEMENTS

This work is partially supported by the NSF under grants 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

Amazon EC2 - Virtual Server Hosting. (2016). Retrieved July 20, 2016, from https://aws.amazon.com/ec2/.

Brustoloni, J. C. (2006). Laboratory Experiments for Network Security Instruction. *ACM Journal on Educational Resources in Computing*, 6(4), Article 5.

Chu, B., Stranathan, W., Cody, J., Peterson, J., Wenner, A. & Yu, H. (2009). Teaching Secure Software Development with Vulnerability Assessment. In *Proceedings of the 13th Colloquium for Information Systems Security Education (CISSE 2009)*, Seattle, WA, 146-150.

Du, W. & Wang, R. (2008). SEED: A Suite of Instructional Laboratories for Computer Security Education (Extended Version). *The ACM Journal on Educational Resources in Computing (JERIC)*, 8(1), Article 3.

EnCase. (2016). Retrieved July 18, 2016, from https://www.guidancesoftware.com/.

Forensic Toolkit (FTK). (2016). Retrieved July 18, 2016, from http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk.

Jackson, L., Lamar, C., Brown, Q., & Latson, V. (2014). Introducing the Big Ideas of Computer Science through a K-12 Teacher Professional Development Workshop. *ASEE Mid-Atlantic Section Fall 2014 Conference*, Swarthmore, PA.

Kizza, J. M. (2006). *Computer Network Security and CyberEthics (2nd.ed.).* Jefferson, NC: McFarland & Company.

Kizza, J. M. (2007). *Ethical and Social Issues in the Information Age (3rd. ed.)*. New York, NY: Springer-Verlag.

Palmer, A. (2005). The Top Ten Most Unusual Computer Forensics Cases. *U.K. Electronic Evidence Newsletter Issue 1 Volume 5*. Retrieved December 21, 2014, from http://www.krollontrack.co.uk/publications/UK_V5_AP_CF.pdf.

ProDiscover Basic. (2016). Retrieved July 18, 2016, from http://prodiscover-basic.software.informer.com/.

Sanders, A. D. (2003). Utilizing Simple Hacking Techniques to Teach System Security and Hacker Identification, *Journal of Information Systems Education*, 14(1) 5-10.

Spears, J. L. & Parrish, Jr., J. L. (2013). IS Security Requirements Identification from Conceptual Models in Systems Analysis and Design: The Fun & Fitness, Inc. Case. *Journal of Information Systems Education*, 24(1), 17-30.

Taclehaimanot, B. & Lamb, A. (2005) Workshops That Work!: Building an Effective, Technology-Rich Faculty Development Program. *Journal of Computing in Teacher Education*. 121(3).

Wagner, P. J. & Phillips, A. T. (2006). A Portable Computer Security Workshop. Journal of Educational Resources in Computing, 6(4).

Yang, L. (2009). Teaching Database Security and Auditing. In *Proceedings of the 40th ACM Technical Symposium on Computer Science Education (SIGCSE '09)*, New York, NY, 241-245.

Yuan, X., Jiang, K., Murthy, S., Jones, J., & Yu, H. (2010a). Teaching Security Management with Case Studies: Experiences and Evaluation, *Journal on Education, Informatics and Cybernetics (JEIC)*, 2(2), 25-30.

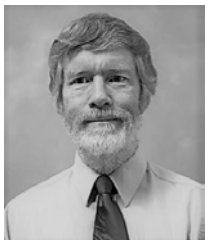
Yuan, X., Vega, P., Qadah, Y., Archer, R., Yu, H., & Xu, J. (2010b). Visualization Tools for Teaching Computer Security. *ACM Transactions on Computing Education (TOCE)*, 9(4).

Yuan, X., Williams, K., Yu, H., Chu, B., Rorer, A., Yang, L., Kizza, J., & Winters, K. (2014). A Workshop on Teaching Information Assurance through Case Studies and Hands-on Experiences, In *Proceedings of the 47th Hawaii International Conference on System Science (HICSS 2014)*, Kona, HI.

AUTHOR BIOGRAPHIES

Xiaohong Yuan is a Professor in the Department of Computer Science and Director of Center for Cyber Defense at North Carolina A&T State University, Greensboro, NC, USA. She received her Ph.D. in computer science from Florida Atlantic University, Boca Raton, Florida. Her research interests include software security, health informatics security and privacy, mobile security, and information assurance education.

Kenneth A. Williams is an associate professor in the Computer Science department of North Carolina A&T State University. He received his Ph.D. from the University of Minnesota and his M.S. and B.S. from Michigan Tech. His research interests include computer science education, novel encryption algorithms, and information security.



Huiming Yu is a Professor and Director of Graduate Study in the Department of Computer Science, North Carolina A&T State University, Greensboro, NC, USA. She received her Ph.D. in computer science from Stevens Institute of Technology, Hoboken, New Jersey. Her research interests include software engineering, visualization, web security, information security, web applications, and cloud computing.

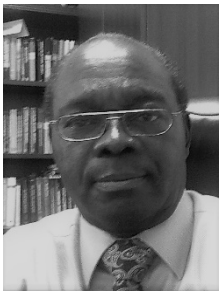
Audrey S. Rorrer is Director of Assessment and Lead Evaluator for the Center for Education Innovation at the University of North Carolina – Charlotte's College of Computing and Informatics. She has been PI, Co-PI, and Senior Personnel on over 20 NSF and Department of Education funded projects. Her research interests include diversity and inclusion in computing education.

Bill Chu is Professor at the Department of Software and Information Systems, University of North Carolina – Charlotte. He is associate director of the Center for Configuration Analytics and Automation. His research interest includes software security, cyber threat intelligence, and security analytics. He received both his B.S. in Electrical Engineering and Ph.D. in Computer Science from the University of Maryland at College Park.

Li Yang is a Professor and Assistant Dean in the College of Engineering and Computer Science. She is the Director of the University of Tennessee – Chattanooga Information Security (InfoSec) Center, a National Center of Academic Excellence in Information Assurance/Cyber Defense (CAE-IA/CD). Her research interests include network and information security, cryptography, intrusion detection, bioinformatics, and engineering techniques for complex software system design.

Kathy Winters is a Distinguished Senior Lecturer in the Department of Computer Science and Engineering at the University of Tennessee – Chattanooga. She has M.S. degrees in Computer Science and Engineering Management, both from the University of Tennesse – Chattanooga. Her research interests are in security with a focus on integration of security throughout the computer science curriculum and security in software engineering.

Joseph M. Kizza is a Professor and Head of the Department of Computer Science and Engineering at the University of Tennessee – Chattanooga. He is on editorial boards of half a dozen scholarly journals and Editor-in-Chief of the International Journal of Computing and ICT Research (IJCIR). He has published extensively in journals and conference proceedings including more than ten books on computer ethics, network security, and cyber ethics.



APPENDIX

Table 3 lists the topics, hands-on labs, and teaching cases presented at the workshop, as well as the websites hosting the materials or references where more information could be found about the materials.

Topic	Labs/Teaching Cases	Website/Reference
Cryptography	Cryptographic Al Algorithms and Mechanism; Attacks On Cryptographic Techniques	https://teaching-ia.appspot.com/labs
Access Control and Database Security	Installing Oracle 11g Database; Using Trojan to Exploit the Vulnerability of Discretionary Access Control (DAC); Implementing MAC to Mitigate the Risk of Trojan	https://teaching-ia.appspot.com/labs
Cloud Security	Establishing a Secure Connection to an Amazon Ec2 Instance	https://teaching-ia.appspot.com/labs
Network Security	Packet Sniffer Simulator; A Learning Tool for Kerberos Authentication Architecture; A Visualization Tool for Wireless Network Attacks; Syn Flood Animated Simulator	http://williams.comp.ncat.edu/ia_visualization_labs/security_visual_tools/vistools.html
	Firewall Simulation Game	http://williams.comp.ncat.edu/firesim/index.htm
	Stack Overflow Visualization and Lab	http://williams.comp.ncat.edu/overflow/teaching.html http://williams.comp.ncat.edu/overflow/labs.html
	Wireless Network Attack Exercises	http://williams.comp.ncat.edu/ia_visualization_labs/wireless%20attack%20labs/wirelessattacklabs.html
Security Management	Incident Response Planning Case Study; Disaster Recovery and Business Continuity Planning Case Study; Hypothetical Computer System Risk Management Case Study; ABC Insurance Company Virtualization Case Study; Security Policy Case Study; Cisco Physical Security Case Study; ADVO Physical and IT Security Case Study	http://williams.comp.ncat.edu/ia_visualization_labs/case%20studies/security_management/smindex.html
Web Security	Vulnerability Assessment for Web Applications	Chu et al. 2009
Security Ethics	Ethical Security Scenarios	https://teaching-ia.appspot.com/labs Kizza, 2006, 2007
Digital Forensics	Using Steganalysis Tools; Cellphone Forensics	https://teaching-ia.appspot.com/labs

Table 3. Web References

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872