Developing a Standardized and Multidisciplinary Curriculum for Digital Forensics Education

Masooda Bashir[1], Roy Campbell[2]
College of Engineering, University of Illinois at Urbana-Champaign

1. INTRODUCTION

As digital information continues to proliferate at an unprecedented rate of billions of data bytes generated every day, society continues to rely on digital devices for a multitude of purposes that all leave behind a heavy digital footprint. Digital forensics (DF) is the science of identifying, collecting, preserving, documenting, examining, analyzing, and presenting evidence from computers, networks, and other electronic devices. It is important to establish a standardized curriculum consistent with the fundamentally multidisciplinary nature of digital forensics to prepare students for the various demands of the field and employment opportunities forecasted to increase by over 20% from 2010 to 2018 (Ismand, 2010). From the point of view of a prospective student, a standardized curriculum gives the dual benefits of simplifying the evaluation of degree options and of increasing the employability of those degrees.

2. MULTIDISCIPLINARY CURRICULUM

The challenge for digital forensics education is to create a multidisciplinary curriculum that accommodates the complex and intersecting disciplines related to this field of study. A necessary foundation for the development of this multidisciplinary program was influenced by challenges to digital forensics education already identified, discussed, and published by Bashir, et.al (2014), Lang, et.al (2014), Al Amro, et.al (2012), Garfinkel, et.al (2011), Walls, et.al (2011), Beebe (2009), Kwan, et.al (2008), Bishop (2008), Craiger, et.al (2007), Armstrong, et.al (2004), and Burnett (1996). Further, our design responded to challenges identified by institutions involved with implementing digital forensics programs. These include: balancing training and education (Cooper et al., 2010; Gottschalk et al., 2005), lack of an adequate textbook on digital forensics (Liu, 2006), finding qualified faculty (Gottschalk et al., 2005; Liu, 2006), lab setup (Gottschalk et al., 2005; Liu, 2006), selecting appropriate prerequisites (Liu, 2006; Chi et al., 2010), and absence of widely accepted curriculum standards (Forensic Science Education Programs Accreditation Commission, 2012; ACM/IEEE-CS Joint Task Force on Computing Curricula, 2013; West Virginia University Forensic Science Initiative, 2007; Scientific Working Group on Digital Evidence, 2010).

3. STANDARDIZED CURRICULUM

Over the past three years at the University of Illinois at Urbana-Champaign we have developed a new undergraduate certificate program and related curriculum for our digital forensics program, with funding awarded by the National Science Foundation[3], and are in the process of revising the curriculum for distribution to other institutions. Our model for a standardized digital education curriculum emphasizes that digital forensics should be a specialization within a technical domain. The curriculum package provides a strong theoretical foundation for the techniques learned by the students as well as an array of studies in fields related to digital forensics. The hallmarks of the program include a multidisciplinary approach to digital forensics education, domain experts from multiple fields related to digital forensics develop and teach the curriculum, and course work is modular and portable. The modular approach to curriculum development is organized by a three-course digital forensics education sequence, and the modules are combined to form a coherent narrative, thus exposing students to multiple perspectives on digital forensics. Domain experts in computer security, computer networks, law, civil and criminal justice, fraud investigation, and psychology took the lead in developing and teaching topical modules focused on their areas of expertise. The modular course content is designed with the intentions of being easily adaptable and integrated at various education institutions. To lower the entry barrier preventing institutions from adopting digital forensics programs, we are designing it as a self-contained curriculum package with everything needed to teach the course. When complete, our program will consist of an introductory and an advanced course in digital forensics, with accompanying hands-on laboratory assignments.

4. WORKSHOPS AND EVALUATION

The high-level student learning outcomes that guided the curriculum development included: (a) introduction to established barriers and challenges in the field; (b) develop investigative skills and techniques applicable to industry; (c) understand digital forensics' limitations; (d) contribute research. To facilitate the construction of an initial curriculum vision, the team developed a series of workshops (the proceedings are now in press) to include experts in the field of digital forensics. Findings and guidance gathered from these workshops significantly added to the curriculum development process. Additionally, an external evaluation team was hired to conduct a formal evaluation of the initiative by providing: (a) ongoing feedback to inform the implementation and delivery of the curriculum; (b) comprehensive assessment of program effectiveness and outcome attainment. Being responsive to the multiple groups of individuals involved with the initiative helps to legitimize a diversity of perspectives and experiences and contribute to a comprehensive understanding of the curriculum being developed. To that end, the evaluation design includes both quantitative and qualitative methods developed in collaboration with the initiative's leadership team.

5. OPPORTUNITIES AND CHALLENGES

Digital forensics education curriculum needs to be developed by taking into consideration the need for students to be aware of the multiplicity of field specializations. A particular challenge for teaching this course sequence results from the broad nature of the field of digital forensics. It is difficult to provide students with the greatest depth of knowledge of a particular aspect of a field that encompasses a wide range of technical topics. Given that multiple modules were necessary to cover the specificities of each topic, one of the challenges of teaching an introductory digital forensics course was to present a cohesive narrative. A challenge particular to developing a security-based curriculum was a higher-level conflict in the balance of training versus education programs. Both programs are necessary to the field and are particularly important in the acknowledgement of the security community. Achieving this balance involves the laboratory assignments of both programs. In many computer science courses, students are not given an opportunity to take information learned and apply it to a lab assignment. Consequently, the challenge involves designing laboratory assignments to offer students unique insight to the materials learned.

Our development of a standardized and multidisciplinary curriculum for digital forensics continues to evolve. During this process, we would like to engage with more researchers in the field to gain their input and knowledge of their experiences and to share our curriculum, what we have learned from its implementation, and our vision for multidisciplinary digital forensics curriculum standardization in the future.

6. REFERENCES

ACM/IEEE-CS Joint Task Force on Computing Curricula. Computer Science Curricula 2013 [Tech. rep.]. ACM Press and IEEE Computer Society Press; December 2013.

Bashir M., Applequist J., Campbell R., DeStefano L., Garcia G., Lang A. Development and Dissemination of a New Multidisciplinary Undergraduate Curriculum in Digital Forensics. Conference on Associate Digital Forensics, Security and Law (ADFSL). Richmond, VA, USA: 2014.

Chi H, Dix-Richardson F, Evans D. Designing a computer forensics concentration for cross-disciplinary undergraduate students. In: Proceedings of the 2010 Information Security Curriculum Development Conference. New York, NY, USA: ACM; 2010. pp. 52e7.

Cooper P, Finley GT, Kaskenpalo P. Towards standards in digital forensics education. In: Proceedings of the 2010 ITiCSE Working Group Reports. New York, NY, USA: ACM; 2010. pp. 87e95.

Forensic Science Education Programs Accreditation Commission. FEPAC accreditation standards [Tech. rep.]. American Academy of Forensic Sciences; 2012.

Gottschalk L, Liu J, Dathan B, Fitzgerald S, Stein M. Computer forensics programs in higher education: a preliminary study. SIGCSE Bull Feb. 2005;37:147e51.

Illinois Science, Technology, Engineering, and Mathematics Education Initiative. Digital forensics course evaluation report [Tech. rep.]. University of Illinois at Urbana Champaign; January 2014.

Kessler, G. C., Schirling, M. E. The Design of an Undergraduate Degree Program in Computer and Digital Forensics. J. of Digital Forensics, Security and Law, 1.3, 37-50 (2006).

Lang A., Bashir M., Campbell R., DeStefano L. Developing a new digital forensics curriculum. In: Digital Investigation 11; 2014, pp. S76-S84.

Liu J. Developing an innovative baccalaureate program in computer forensics. In: Proceedings of the 36th Annual Frontiers in Education Conference; 2006. pp. 1e6.

Meyers, M., Rogers, M. Computer Forensics: The Need for Standardization and Certification. International Journal of Digital Evidence, 3.2, 1-11 (2004).

Nance, K., Armstrong, H., and Armstrong, C. Digital Forensics: Defining an Education Agenda. System Sciences, HICSS, 2010, 43rd Hawaii International Conference. pp. 1-10. IEEE (2010).

Scientific Working Group on Digital Evidence. SWGDE/SWGIT guidelines and recommendations for training in digital and multimedia evidence [Tech. rep.]. Scientific Working Group on Digital Evidence; January 2010.

Srinivasan S. Computer forensics curriculum in security education. In: Proceedings of the 2009 Information Security Curriculum Development Conference. New York, NY, USA: ACM; 2009. pp. 32e6.

Woods, K., Christopher Lee, Simson Garfinkel, David Dittrich, Adam Russel, Kris Kearton, Creating Realistic Corpora for Forensic and Security Education. ADFSLConference on Digital Forensics, Security and Law (2011).

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., Sommer, P. M. Computer Forensics Education. IEEE Security and Privacy, vol. 1.4, pp. 15--23 (2003).

[1] Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign, https://www.lis.illinois.edu/people/faculty/mnb

[2] Computer Science, University of Illinois at Urbana-Champaign, http://cs.illinois.edu/directory/profile/rhc

[3] http://www.nsf.gov