INFORMATION SYSTEMS EDUCATION JOURNAL

Volume 17, No. 6
December 2019
ISSN: 1545-679X

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is six times per year. The first year of publication was 2003.

ISEDJ is published online (http://isedj.org). Our sister publication, the Proceedings of EDSIGCON (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the EDSIGCON conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for ISEDJ.

Certifying Business Students in Microsoft Office Specialist Certification Excel Core Exam: Lessons Learned

Nesrin Bakir
nbakir@wtamu.edu

Kareem Dana
kdana@wtamu.edu

Amjad Abdullat
aabdullat@wtamu.edu

West Texas A&M University
Canyon, TX 79016

Abstract

Data analytical skills are essential to compete in today's competitive economy. The ability to understand, use, codify, and manipulate data to make business decisions is an essential factor of information competence. One way to ensure that students are well-prepared in terms of their technological literacy is through the use of certifications in course offerings. This paper details the process of providing the Microsoft Office Specialist Excel Core Certification Exam to students in our Computer Information Systems program. We discuss how we integrated the certificate program into our curriculum, the necessary pedagogical changes, and technologies used. We also review our successes, pitfalls, and results.

Keywords: Certification, Microsoft Excel, Analytical Skills, Pedagogy, GMetrix SMS

1. INTRODUCTION

Technological literacy is essential to compete in today's economy. The ability to understand, use, and manipulate data to make decisions is an essential factor of information competence (Mandinach & Gummer, 2013). One way to ensure that students are well-prepared in terms of their technological literacy is the implementation of certifications into course offerings. These types of technology skill-based courses are well-established at business schools across the nation. Additionally, certificate programs are becoming more popular in Computer Information Systems (CIS) curricula. Furthermore, the Association to Advance Collegiate Schools of Business (AACSB) has stated that technology in business curricula is a near necessity and graduates need to have the ability to "leverage technology in a scalable fashion to advance firms' strategies and operations" (AACSB, 2002, p. 11). Research has shown that business students benefit from earning IT-based skill certifications (Gomillion, 2017). AACSB has also indicated a shift towards relevant skills such as Microsoft Excel in hiring of business school graduates (Gomillion, 2017). Several research papers note that advanced analytical skills, Excel, in particular (such as those taught by MyEducator (MyEducator, 2018) and certificate programs) result in increased marketability and increased compensation for graduates (Formby, Medlin, & Ellington, 2017). General knowledge of Excel that students may obtain outside of the classroom is no longer sufficient. Over 80% of business students claim their goal is to get a good paying job, and many businesses are requiring advanced Microsoft Excel skills (Formby et al., 2017).

Our college is a regional, AACSB accredited business school. To prepare students for successful careers with skills relevant to marketability and employability, we began offering the Microsoft Office Specialist (MOS) Excel Core Certification Exam during the Fall 2017 semester. The certificate was offered across two courses and three sections each semester during the 2017-2018 academic year as a pilot program. The goal of the pilot was to learn what it takes to implement the MOS certification smoothly regarding curricula, technology requirements, and cost with a longer-term goal to require all College of Business students to get certified.

MOS includes three levels of certification: Specialist, Expert, and Master. We chose to use the Specialist certification based on the needs of our students and to ensure that the students have the core skills with Microsoft Excel. The MOS certification measures and validates Excel core skills in five topics: (a) create and manage worksheets and workbooks; (b) manage data cells and ranges; (c) create tables; (d) perform operations with formulas and functions; and (e) create charts and objects. We decided to implement the certification program for three reasons: (a) provide students with industry-recognized certification, (b) improve students' current and future employment options, and (c) provide a competitive advantage to our college and department.

The purpose of this paper is to detail the process of providing the MOS Excel certificate to students in our Computer Information Systems program. We discuss how we integrated the certificate program into our curriculum, the necessary pedagogical changes made, and technologies used. We also review our successes, pitfalls, and results.

2. BACKGROUND

According to Randall and Zirkle (2005), entry-level certification is a "vehicle to provide students with viable skills needed by the workforce" (p. 287). Certifications are also confirmation of adequate knowledge and skills (Cantor, 2002) and provide students with credentials that are recognized by business and industry (Association of Career and Technical Education, 2015). Certifications have a significant effect on the employability of employees (Certiport, 2015; Chilton, Hardgrave, & Armstrong, 2010; Dubie, 2010; Hunsinger & Smith, 2009; Quan & Cha, 2010). These certifications also prepare students to compete in competitive job markets and showcase their marketability while they are still in school. According the Certiport (a Pearson VUE business to administer the certifications), the national average pass rate for the Microsoft Office Specialist Excel certificate is 63% on the first attempt (Tastle, Mead, Rebman, Marks, & Phillips, 2017). Based on the Pearson VUE Value of IT Certification survey (2016), findings showed employees benefitted from acquiring a certification. For example, 65% of the employees indicated a positive impact on their professional image, 20% received a salary increase, 19% found a job, and 14% received a promotion. The certificate sends a positive signal to potential employers (Gomillion, 2017). Research shows that 67% of all middle-skill job openings require at a minimum proficiency in productivity software such as Microsoft Excel and pay 13% more than those that don't (Burning Glass Technologies, 2015). However, a recent report conducted by the Manpower Group (2016-2017) revealed that 40% of the employees had difficulty filling these middle-skill jobs. Lastly another research paper (Formby et al., 2017) quotes Andrew Soergel (2015) as stating that "Jobs requiring advanced analytical tools skills offer the strongest opportunity for middle-skill job seekers in terms of salary and growth as well as career advancement. Effectively, entire segments of the U.S. economy are off-limits to people who don't have basic analytical skills."

Several higher education institutions have found success in the implementing Microsoft Office Specialist (MOS) certification program into their curriculum. The higher education success story case studies conducted by Certiport (2017) revealed highly positive outcomes. For example, the implementation of MOS Excel and PowerPoint at the Daniels College of Business at the University of Denver improved student performance, enriched recruiting power, improved student placement, and expanded the program. Incorporating the certification program allowed Richland College's School of Engineering, Business, and Technology program to provide students with recognized workforce credentials as well as establish and grow their program. The benefits of MOS at Tulane University's Freeman School of Business included improved student performance and enhanced institutional reputation and recruiting power.

3. IMPLEMENTATION

We began the certificate program in the Fall 2017 semester. The initial launch of the certification program required significant ground work: buying the campus licenses for GMetrix (GMetrix Skills Management System, 2018) and Console 8, the Certiport exam delivery software, working with the Information Technology (IT) office to install the required software, filling out paperwork for accessibility, reserving labs, training instructors and proctors, and modifying course content. Since our school was already a Certiport Authorized Testing Center, we were ready to offer the certification exam on campus. We piloted the certification in two different courses in the CIS department–Introduction to Information Systems and Management of Information Systems (MIS). This was to help determine which course would be the best long-term fit for the MOS certificate. We also chose these courses because both already included Microsoft Excel content. The Introduction to Information Science course is part of the university core and open to all students without prerequisites. Many of the students were underclassmen and had either no or limited Excel experience. The MIS course, on the other hand, is required for all business students and is mostly upperclassmen. Even though we did not survey students' Microsoft Excel skills, our experiences showed that students in the MIS courses usually have a wider variety of Microsoft Excel and general computer skills. Students take the MIS course later in their program and after completing a pre-requisite course in statistics where they are introduced to Microsoft Excel basics. The content of both courses was heavily modified to accommodate the certificate curriculum.

We used GMetrix SMS (GMetrix Skills Management System, 2018), a web-based system, to prepare students for the exam in addition to the instructor prepared materials. The GMetrix practice tests are performance-based and provide a simulation of the actual exams. As students practice their skills on these tests, they build confidence, enhance their learning, and become familiar with the testing environment prior to the actual exams. GMetrix practice tests offer both testing and training modes. The testing mode provides timed practice tests that simulate actual tests, while the training mode provides self-paced learning experiences that provide students with feedback and step-by-step instructions for each skill. The questions are the same for both modes. GMetrix contains six Microsoft Excel exam modules. Students were required to complete four modules with a score of 95% or better on each module in testing mode. Students received a detailed rubric upon completion which highlighted the skills requiring additional review. Students had only one attempt to take the certification exam. The MOS Certification Excel Core exam is 50 minutes. Students need a score of 700 out of 1000 to pass. In the introductory course, the GMetrix assignments and the certification exam counted for 25% percent of the final grade, in the MIS course, it was 10% for the assignments and 20% for the certificate exam.

Roughly the same amount of in-class time was spent on each topic, but students were able to spend more time on specific topics most challenging to them, if they chose to. Some students completed a GMetrix assignment just once, while other students practiced several times. This capability of GMetrix was helpful in handling the wide variety of student knowledge and skills with Microsoft Excel.

While Certiport's Console 8 software is required to administer the MOS exam, GMetrix is one of several options available to prepare for the exam. Other universities have used options such as Pearson MyITLab, Lynda.com, textbooks, or in-class instructions (Tastle, Mead, Rebman, Marks, & Phillips, 2017). We chose GMetrix after careful consideration. GMetrix closely mirrors the MOS exam format and curricular needs. GMetrix also allowed the instructors to create training materials specific to student needs.

Description of Introduction to Information Science Course

Our Introduction to Information Science course is an introductory three-credit hour course (1 hour and 15 minutes twice a week) that teaches Microsoft productivity tools, digital literacy, basic computer operations, and coding to enhance students' ability to retrieve, synthesize, evaluate, and communicate information. The Microsoft Word, Excel, and PowerPoint portion of the curriculum provides critical instruction to develop technological skills to assist students in communicating, evaluating, and presenting information throughout their academic and professional lives. Although the previous curriculum tested students' mastery of the Microsoft Office productivity tools, it did not provide certification that students were career ready. This class is conducted in a computer lab where each student has a PC computer.

During the Fall 2017 semester, students were given six class sessions for exam preparation and completed two GMetrix assignments per week. The exam preparation included instructor-led demonstrations of Microsoft Excel skills where students followed along at their computers. Due to different student Microsoft Excel skills and knowledge, the instructor set-up various learning activities where students chose which skills they needed to focus more on and practice. This method allowed students to build on their skills and knowledge at their own pace. To minimize the cost for the students, the textbook requirement was eliminated. Instead, students purchased a required voucher from the university bookstore that allowed access to GMetrix and Console 8 software programs.

Students were given two weeks to complete four GMetrix assignments in the testing mode. They were encouraged to work on the training mode for each assignment. This option allowed them to work on their own pace and receive step-by-step instructions for each question when needed.

Description of Management of Information Systems Course

Management of Information Systems (MIS) is a three-credit hour course that is required for all business students in the College of Business. This course focuses on general management information systems including topics such as how I.S. impacts organizations, ethical considerations of I.S., challenges, emerging trends, and global nature of information systems. The course activities include case studies, lectures, videos, group project, and Microsoft Excel and Access assignments using MyEducator (MyEducator, 2018). MyEducator is an online textbook with interactive lessons and modules on Microsoft Excel and Microsoft Access. Ten Microsoft Excel modules and three Microsoft Access modules were taught. To accommodate the certificate the Microsoft Access modules and group project were removed. This freed up the final three weeks of the course. This class is conducted in a regular classroom where students are encouraged to bring their laptops. Students in this class purchased the MyEducator e-Book but did not pay for GMetrix or the exam voucher. These were provided by the College of Business.

Fall 2017 Results

A total of 132 students took the exam across the three courses (two sections of MIS). 61% percent of the students passed, 29% did not pass, and 10% did not take the certification exam. Table 1 summarizes the overall pass and fail rates across three classes.

Course	Enrolled	Passed	Failed	Not Taken
Intro IS	40	20 (50%)	14 (35%)	6 (15%)
MIS Section 1	61	41 (67%)	15 (25%)	5 (8%)
MIS Section 2	31	20 (65%)	9 (29%)	2 (6%)
Total	**132**	**81 (61%)**	**38 (29%)**	**13 (10%)**

Table 1: 2017 Certification Results

Our results are slightly below the national average of 63% who pass on their first attempt.

Spring 2018 Implementation Changes

Based on the previous results, we decided to make changes to our implementation approach and revised the curriculum for both courses. We added more class periods for Microsoft Excel examples and demonstrations to complement the GMetrix SMS modules. We also added custom GMetrix modules, custom-authored Microsoft Excel examples and demonstrations, and more in-class instruction. The following is a list of the instructional design changes we incorporated into the curriculum:

1. Students were given more time to complete the GMetrix assignments. Instead of six, we scheduled ten class sessions for GMetrix SMS practice. This allowed students to complete one GMetrix assignment per week instead of two.

2. The instructors used custom-authored examples to demonstrate ALL certificate exam learning objectives throughout the semester. This included four different Microsoft Excel workbooks and over 135 lecture slides of the certificate topics.

3. We still conducted instructor-led demonstrations and made sure that the instructors demonstrated each skill that could be on the exam. The instructors also reviewed the weekly GMetrix assignment in class with the students in the training mode first. Then, students completed the assignment in the testing mode on their own. Students responded positively to this instructional method and customized GMetrix exercises.

4. GMetrix SMS allows instructors to create custom modules. We created eighteen modules on specific certification exam learning objectives such as conditional formatting, sparklines, tables, and functions.

These modules were not graded, but students were encouraged to take them as many times as necessary for practice. This helped with students' different levels of Microsoft Excel skills as each student was able to spend more time on topics of their choice at their own pace and build their confidence.

Spring 2018 Results
A total of 129 students took the exam in Spring 2018. Seventy-one percent of the students passed, 25% did not pass, and 4% did not take the certification exam. Table 2 summarizes the overall pass and fail rates across three classes.

Course	Enrolled	Passed	Failed	Not Taken
Intro IS	37	30 (81%)	7 (19%)	0 (0%)
MIS Section 1	59	35 (59%)	18 (31%)	6 (10%)
MIS Section 2	33	26 (79%)	7 (21%)	0 (0%)
Total	**129**	**91 (71%)**	**32 (25%)**	**6 (4%)**

Table 2: 2018 Certification Results

Compared to the previous semester, we saw a 10% improvement. Introduction to Science course saw a 31% improvement in passing. MIS Section 2 saw a 14% increase, while section 1 saw a decrease of 8%. We credit the improvements to the changes made. MIS Section 1 had the most students and was not taught in a computer lab and had some students who did not take the exam. Those challenges may have contributed to the noted performance despite the implementation changes. Table 3 shows a summary of the results students received both semesters.

Course	Enrolled	Passed	Failed	Not Taken
Intro IS	77	50 (65%)	21 (27%)	6 (8%)
MIS Both Sections	184	122 (66%)	49 (27%)	13 (7%)
Total	**261**	**172 (66%)**	**70 (27%)**	**19 (7%)**

Table 3: Summary of Results Both Semesters

4. LESSONS LEARNED/IMPLICATIONS

The pilot study was a success. We learned many lessons detailed below that will enhance our college wide expansion of the certificate program. Based on the lessons learned from our approach during the Fall 2017 semester, we were able to incorporate many changes into the curriculum which allowed us to gain better results in our implementation efforts. We categorized the lessons in four areas: course, technology, IT, and cost related.

Course Related
Scheduling more class time, custom GMetrix modules, custom-authored Microsoft Excel examples and demonstrations, and more in-class instruction allowed students to better absorb the material. We found that having the class taught in a computer lab was beneficial because this allowed students to follow along with the instructor. Introduction to Information Systems was taught in a computer lab and saw the biggest improvement in scores, whereas our MIS course was not. Also, MIS Section 1 had 61 and 59 students each semester respectively. According to the instructor, that large number of students proved to be a challenge in such a hands-on skills-based course in a regular classroom. We plan to add more sections of the course in a computer lab to mitigate this problem.

Because GMetrix is a Windows-based program, Mac users could not use their personal laptops to work on the assignments or complete the hands-on assignments outside of class. This required students to come to campus and work on these assignments. This created some challenges for students who had to juggle a family and professional lives. For students who worked on their own laptop to complete the GMetrix assignments, some ran into technical problems, bugs, and crashes caused by their computer system or the GMetrix software.

Despite these minor pitfalls, we believe GMetrix is a useful tool to prepare the students for the certificate exam and plan to continue using it. Overall, it prepares the students well for the exam. Coupling GMetrix with our own custom modules and instruction helped increase our students' pass rate. However, we did find that GMetrix scores alone may not predict success on the certificate exam. Some students who did very well on GMetrix, did not pass the exam. The GMetrix training mode provides step-by-step answers that some students may have memorized and then repeated in testing mode without proper understanding of the concepts. It may be more helpful to students if GMetrix training questions and testing questions have some differences. We also found that some students experienced exam anxiety.

Management of Information Systems used MyEducator while Introduction to Information

Science did not. MyEducator is helpful in teaching Microsoft Excel; however, many of the MyEducator topics are not directly relevant to the certificate exam. After making course improvements in the Spring 2018 semester, we found that MyEducator did not lead to better certificate test scores. MyEducator does not claim to prepare students for the certificate exam and instead teaches more advanced skills such as pivot tables, optimization analysis, and others. While these skills are not on the certificate exam, they remain useful for business students. We plan to continue using MyEducator and will re-evaluate where it fits in within the context of the certificate exam in the coming semesters.

Student feedback was generally positive based on course evaluations. Across the three courses, most feedback noted that the students found the Microsoft Excel skills and certificate helpful. The following are some of the comments students shared:

- "Content was excellent, resources were more than adequate to fill students' needs…The subject is not only relevant, but directly beneficial to students taking the course,"

While some students found the technologies used useful, some comments revealed students were not happy with GMetrix. Below are some of the student comments:

- "Online practices have shown me many aspects of excel I had not used before and didn't know how to use until now,"
- "G-metrix good system for preparing for excel,"
- "Gmetrix was hard to deal with at times," and
- "Gmetrix part of course is outdated and incompatible with most computers and makes homework extremely difficult."

Further feedback included a desire for even more in-class time to prepare for the exam– "I felt very limited on time." and "Just felt limited and crammed." This feedback is helpful to evaluate the success of the pilot and will guide us to make the necessary changes in the future.

Technology Related Problems During Exam

During Fall 2017, three students encountered technical problems where they had to restart the exam. Through the help of the Certiport technical support, the issues were resolved, and the students were able to complete the exam. During Spring 2018, only minor problems were reported during the exam that were able to be resolved without losing any exam progress. We are aware that some technical problems are not predictable and recommend that any university considering implementing the certificate program have a technical support plan. For us, this consisted of having Certiport technical support on speed dial and having our IT department on hand to fix any computer crashes or freezes during the exam. We also made sure that the day before the exam, one of the instructors took the exam to ensure that the technology was working properly.

IT Related

Implementing the certificate program required close coordination with the University's IT department. We requested that our IT department install, maintain, and update the GMetrix SMS and Console 8 software on the lab and instructor computers. We also worked with IT to be on hand during the certificate exam days to provide immediate technical support in case of a problem during the exam itself. Being a pilot program, this was new to both IT and the instructors. Constant communication with IT staff and testing helped make this aspect successful. We encourage other universities to have an assigned IT personnel for this and not to overlook the importance of working closely with IT to implement a certificate program.

Cost Related

One often overlooked aspect of implementing the certificate exam is the financial cost to the students and the university. As of June 2018, the list price for a single Microsoft Office Specialist Exam Voucher is $96.00. GMetrix practice tests cost $40.00 (Certiport, 2015). We chose to purchase a GMetrix campus license and Certiport MOS exam campus license at a discounted rate of $6,930.00 (GMetrix license $3,150.00 and MOS campus license $3,780.00). The MOS campus license came with 500 vouchers and expires a year from the purchase date. There are many different approaches that universities can take regarding this financial aspect. In fact, we took a different approach with our two courses. Students in the MIS course purchased the MyEducator eBook but did not have to purchase anything else. They were provided with an exam voucher and a GMetrix code through our campus license for no additional cost. Introduction to IS students did not have to purchase a textbook but in exchange purchased an exam voucher for $70.00. This voucher covered both access to a GMetrix code and an exam voucher. We partnered with the bookstore where students bought the voucher, and the funds were transferred to a College of Business account at the end of each semester. Students did appreciate that the cost of the certificate was subsidized, and this approach worked for our university.

6. CONCLUSIONS

The purpose of this paper is to provide insights to other educators who might be interested in the implementation of the MOS certification in their program. Our attempt showed us that students benefit from having more time to master the skills, apply their knowledge, and become comfortable with the materials and exam. Students also benefited from the increased in-class instruction and teacher demonstrations. As we continue to incorporate the certification, we are certain that we will continue to modify the curriculum based on student and college needs. Another area we will focus on is to understand how students' Microsoft Excel knowledge and skills change throughout the semester. We will survey students about their skills before and after they go through the training. This will allow us to track student knowledge and skills. We hope that the lessons we learned from this pilot program will be useful to assist others who are interested in adopting the certification exam. In the future, we plan to follow up with our graduates to see if the certification has helped them get a job or a promotion. We also plan to roll out the certificate program to all our College of Business students in the coming years.

9. REFERENCES

AACSB (2002). Management Education at Risk. Retrieved from https://www.aacsb.edu/-/media/aacsb/publications/research-reports/management-education-at-risk.ashx?la=en

Association of Career and Technical Education (2015). CTE: Information and Research. Retrieved from http://www.acteonline.org/cteresearch

Burning Glass Technologies (2015). Crunched by the numbers: The digital skills gap in the workforce Retrieved from http://burning-glass.com/research/ digita1-skills-gap/

Cantor, J. (2002). Skills certifications and workforce development: Partnering with industry and ourselves. *Leadership Abstracts,* 15(1), 2-4.

Certiport (2017). Microsoft Office success stories. Retrieved from https://certiport.pearsonvue.com/Certifications/Microsoft/MOS/Success-stories

Certiport (2015). Retrieved from https://certiport.pearsonvue.com/Certifications/Microsoft/MOS/Overview

Chilton, M. A., Hardgrave, B. C., & Armstrong, D. J. (2010). Performance and strains levels of IT workers engaged in rapidly changing environments: A person-job fit perspective. *ACM SIGMIS Database,* 41(1), 8-35.

Dubie, D. (2010). IT certifications worth more now as economy grows. *Network World,* 27(8), 1-1,12.

Formby, S. K., Medlin, D., & Ellington, V. B. (2017). Microsoft Excel®: Is It An Important Job Skill for College Graduates? *Information Systems Education Journal, 15*(3), 55-63.

Frydenberg, M. (2013). Flipping Excel. *Information Systems Education Journal, 11*(1), 63-73.

GMetrix Skills Management System. (2018, June 10). Retrieved from http://www.gmetrix.net

Gomillion, D. L. (2017). The Role of IT Industry Certifications in an AACSB-Accredited Institution. *Information Systems Education Journal, 15*(1), 68-79.

Hunsinger, D. S., & Smith, M. A. (2009). IT certification use by hiring personnel. *The Journal of Computer Information Systems, 50*(2), 17.

Mandinach, E., & Gummer, E. (2013). A Systemic View of Implementing Data Literacy In Educator Preparation. *Educational Researcher, 42*(1), 30-37.

Manpower Group 2016-2017, Talent Shortage Survey. Retrieved from http://manpowergroup.com/talent-shortage-2016.

MyEducator. (2018, June 10). Retrieved from http://www.myeducator.com

Randall, M. H., & Zirkle, C. J . (2005). Information technology student-based certification in formal education settings: Who benefits and what is needed. *Journal of Information Technology Education, 4,* 287-306.

Soergel, A. (2015, March 5). *Want a Better Job? Master Microsoft Excel.* Retrieved from http://www.usnews.com/news/blogs/data-mine/2015/03/05/want-a-better-job-master-microsoft-word-excel

Tastle, W., Mead, C., Rebman, C., Marks, S., & Phillips, K. (2017). Building Excel Expertise: A Guide in Best Practices. *Proceedings of the EDSIG Conference.* ISSN: 2473-3857 v3 n4326.

The Pearson VUE Value of IT Certification survey (2016). Retrieved from https://home.pearsonvue.com/Documents/Marketing/2016-Pearson-VUE-Value-of-IT-Certification-Survey_.aspx

Intellectual Merit and Broader Impact: Collaborative Education toward Building a Skilled Software Verification and Validation Community

Sushil Acharya
acharya@rmu.edu
Department of Engineering

Priyadarshan A. Manohar
manohar@rmu.edu
Department of Engineering

Peter Y. Wu
wu@rmu.edu
Department of Computer and Information Systems

Robert Morris University
Pittsburgh, PA 15108

Abstract

Software Verification and Validation (SV&V) is proven to be an effective approach to ensure software quality. Yet it is not commonly deployed in industry practices. We started a project intent on building a sustainable community skilled in SV&V. The fundamental objective is the transformation of undergraduate education in software engineering. The project involved collaborative partners in both industry and academia. Through the discussions in focus groups, the curriculum for SV&V was vigorously reviewed, checking against the best practices in industry while identifying and prioritizing gaps. The project went on to develop new active learning tools along with outcomes assessment instruments, designed to enhance delivery and retention of knowledge in SV&V, both theoretical and practical, specifically in the areas of requirements management, software reviews, configuration management and software testing. The project resulted in 44 delivery contact hours of teaching modules using these active learning tools: case studies, class exercises and case study videos. The deliverables of the project have been shared, refined and disseminated through training workshops attended by our academic and industry partners, and are now publicly available online. The paper presents the project, and sums up on how the project achieved the goals of intellectual merit and broader impact, which are the criteria based on which the supporting agency National Science Foundation evaluated the project proposal.

Keywords: Software Engineering Education, Software Verification and Validation, SV&V, Active Learning Tools, Intellectual Merit, Broader Impact.

1. INTRODUCTION

Software Verification and Validation (SV&V) is proven to be effective in ensuring software quality and yet only rarely used in industry (Arthur, Groener, Hayhurst & Holoway, 1999; Wang, Ostroff & Hudon, 2014), we started a project intent on building a sustainable community skilled in SV&V. The goal was aimed at the direction of transforming undergraduate education in software engineering. The project involved partners in industry and academia in collaborative education. Armed with the joint partnership, we vigorously reviewed the SV&V curriculum, checking for gaps against industry best practices.

The knowledge areas listed in the IEEE/ACM (2014) Software Engineering Curriculum Guidelines encompass both theoretical and practical aspects pertinent to SV&V practices in industry. These knowledge areas are essential for undergraduate education and a subsequent professional career in software engineering. The dearth of SV&V practitioners in industry seems to indicate the ineffective pedagogy with regards to these knowledge areas (Arthur, Nance, Joines, Barton, Kang & Fishwick, 2000). We therefore set our goal to create new tools to engage the students in active learning of SV&V. Iterative refinement and re-development of the active learning tools would need the support of a collaborative partnership. Dissemination of the new pedagogy and networking to promote the deployment of the new tools aimed at building a community skilled in SV&V.

Our research proposal was awarded an NSF grant for the TUES (Transforming Undergraduate Education in STEM) program in 2013 to address the SV&V pedagogical issues. The project was funded for three years followed by the approval of one year no-cost extension. Many academic and industry partners were involved at various levels of collaboration and participation. Guided and guarded by the industry and academic partnership, we developed new SV&V learning tools. Through training workshops, we not only iteratively refined and re-developed the learning tools as well as the delivery strategies, we also further disseminated the new learning tools and broadened the partnership to implement the new teaching approach through networking. The new learning tools were first shared with the partners and are now publicly available.

This paper reports our effort in the project and present a summary outline, categorizing the new teaching tools now available. Section 2 presents the overall goal and the objectives, followed by a discussion of the partnerships and their roles involved in the project. Section 3 proceeds on to describe how the partners were organized into focus groups to critically review the existing SV&V curriculum and pedagogical approach. Section 4 explains the active learning tools and how they may engender active learning. The development methodology of the new learning tools is also described. One example from each category of the Active Learning Tools is shared briefly in our discussion. Three tables list all the Active Learning Tools from the project in their appropriate categories. Section 4 closes with discussing the appropriate delivery strategies for the new teaching approach. Section 5 describes the SV&V training workshops to refine and promote the learning tools with an even broader invitation to the partnership. Section 6 presents the two web portals to access the project deliverables – the active learning tools. Sections 7 and 8 sum up the achievements of the project to meet the evaluating criteria of NSF, namely, intellectual merit and broader impact. Section 9 presents a summary of the paper.

2. THE PROJECT AND THE COLLABORATIVE PARTNERSHIPS

The goal of our project was to enhance and transform undergraduate education in SV&V by incorporating academic research and industry best practices through collaborative partnership. The following description lays out the progressive objectives to achieve our project goal.

1. To critically review the existing SV&V course content, checking against best practices.
2. To identify gaps and priorities to indicate areas for improvement in pedagogy.
3. To design and develop new materials and active learning tools.
4. To modularize the active learning tools and integrate them into the SV&V course.
5. To develop appropriate delivery strategies for the active learning tools.
6. To evaluate the SV&V course for pedagogy and to formulate assessment instruments.
7. To disseminate the tools for deployment and feedback through networking.

Academic Partners

The project involved two categories of academic partners: development partner and implementation partner. Two institutions were development partners. They were Virginia State University and Milwaukee School of Engineering. Together with the authors' host institution, they carried out the following tasks.

- Joined in the focus groups to critically review the SV&V curriculum.
- Took part to co-develop new course modules to address the gaps in the course content identified by the focus groups.
- Performed assessment of course contents through at least two delivery cycles.

There were six implementation partners: Embry-Riddle Aeronautical University, Montana Technological University, University of Michigan at Dearborn, Virginia State University, Fairfield University, and Milwaukee School of Engineering. Together with the authors' host institution, they carried out the following tasks.

- Used the entire or parts of the courseware developed by the project in at least one course, through at least two delivery cycles.
- Performed assessment of the instruction to evaluate the course.

Industry Partners

The project involved four industry partners. They were either software companies or companies with large software development activities. Their key areas of business included banking, electrical meters, mortgage, pricing and revenue management. They were PNC Bank, Eaton Electrical Corporation, Service Link Inc. and JDA Software Group. The industry partners took part to carry out the following tasks.

- Helped in the focus groups to critically review the SV&V curriculum, checking with industry practices to identify gaps.
- Assisted in the definition and development of new course materials and tools.
- Delivered industry expert lecture sessions as guest lecturer for the SV&V course at the authors' institution.

3. CRITICAL REVIEW OF THE SV&V CURRICULUM

To critically review the SV&V curriculum, we organized the project partners into focus groups. Since strong academia-industry partnership was critical to the project, each focus group comprised of at least one industry partner and one academic partner as members. Each group was assigned one or more SV&V topics for review and discussion, and was led by the project PI and/or co-PIs. The focus groups met once every year at the authors' institution and twice a year in teleconference through various media, in addition to ad hoc virtual online meetings and discussion groups. The activities facilitated for educators and practitioners to understand one another while sharing their thoughts about the SV&V curriculum under review.

The practice of SV&V is well known in the software industry since the 90's (Pham, 1999). Listed in the knowledge areas of the standard curriculum guidelines, SV&V is an essential part of undergraduate software engineering curriculum (IEEE/ACM, 2014). It encompasses both theoretical and practical aspects of knowledge pertinent to a professional career. The knowledge areas were well defined, but the students were rarely well engaged in class. The common sentiment in the focus groups was that the application values of SV&V education were generally not made sufficiently obvious to the students. SV&V education was not effectively delivered, festered with non-coverage by the instructors or non-retention by the students of key knowledge areas.

To sharpen our focus in the review, the SV&V topics for the groups were organized into the four specific areas of software engineering, listed namely in the following:

- Requirements Management
- Software Review
- Configuration Management
- Software Testing

Instead of the traditional teacher-centric classroom, we needed new materials and tools as SV&V courseware to improve SV&V pedagogy. The new courseware should aim at engaging the students in active learning. The critical review of the focus groups therefore called for new active learning tools to cover SV&V topics in each of the four specific areas of software engineering listed above. Active learning being required for the students, the intended goals of the tools were the following:

- To incorporate both theory and practice into the SV&V topics.
- To preserve a sense of practical value in real applications when working through design and development details.
- To engage the students in interaction, with questions in class to stimulate thinking and discussion.
- To engender familiarity with industry practices and enhance understanding even when undergraduate students often lacked the experience.

The active learning tools to be developed were case studies, class exercises and case study videos. For each of the four areas of software engineering, we developed these new tools. They were intended generally for all the goals stated above, but each type of tool could also be more specific about what it aimed it. Briefly stated, the case study maintained the big picture of a real application while we might get into its details, bringing out the sense of practical value in a real application. The class exercise consisted primarily of discussion questions around a topic. But the questions were designed for stimulation as an invitation to interact. The case study video could engage the viewer in an immersive experience. The next section will discuss each of the active learning tools in further details, and briefly describe the development methodology.

4. THE ACTIVE LEARNING TOOLS (ALTs)

By active learning, we mean tools to build an environment for the teachers and the students to be actively engaged in the course content. They may interact through discussion, problem-solving, critical thinking, debate, or a host of other interactive activities. Active learning requires the student to be doing something other than listening and taking notes (Prince, 2004). In the project, we planned to achieve that by complementing the lecture materials with case studies, class exercises, and case study videos. We called these materials the Active Learning Tools (ALTs).

Case Studies

Case studies are useful tools to teach applications of science and engineering principles. They are effective to contextualize theoretical concepts (Davis & Wilcock, 2003). Many studies also showed the benefits of interactive learning strategy in case studies, shifting the emphasis from teacher-centered to more student-centered activities (Grant, 1997; Raju & Sankar, 1999; Sivan, Wong, Woon & Kembler, 2001). The case studies in our project were primarily drawn from present industry SV&V practices. Students were provided industry standard documents for review to prepare themselves for their tasks. These would involve resolution of review conflicts in the Software Requirements Specification document, or compliance to security standards, or drafting of testing plans from use cases. Our project developed, implemented, and disseminated 12 case studies (Manohar, Acharya, Wu, Hansen, Ansari & Schilling, 2015). Each case study included the case study description, instruction notes, student handout, and assessment instrument.

To briefly share one of the Case Studies, we take an example under Requirements Management. In Module RM17, the fictitious Handsome, Inc. is a company that sells men's clothing and wishes to build its first web site to sell online. While the case study provides the situation for students to solicit user requirements, the learning objective is about identifying and resolving ambiguities in the requirements statements. The supposedly real situation becomes more engaging to the students and provides the context to learn the principles behind the need for requirements to be unambiguous. More in-depth discussion of the case studies is presented in Manohar, et al (2015). Table 1 below lists the entire collection of Case Study Modules in the project, and they are all accessible at the courseware repository discussed in Section 6.

SV&V Area	Case Study	mins
Requirements Management	Understanding User Requirements	50
	Requirements from a Customer's Perspective	250
Configuration Management	Continuous Integration	100
	Version Control Management System	100
Software Reviews	Importance of Reviews	100
	Peer Review Tools	100
Software Testing	Test Case Development	50
	Performance Testing/ Load Testing	50
	Software Test Plan (STP)	100
Additional Topics	Liability for Bad Software and Support	50
	Software Legal Issues	50
	TOTAL	1000
	Contact hours (in 50 min periods)	20

Table 1. Case Study Modules

Class Exercises

Class exercises provide activity during class time to explicitly raise questions that invite student participation. Woods and Howard (2014) effectively used class exercises for information technology students to study ethical issues. Day and Foley (2006) used class time exclusively for exercises, having their students to prepare beforehand for class with materials provided online. Frydenberg (2013) primarily used hands-on exercises to foster student understanding in data analytics. Based on the context of the class module, class exercises may involve questions to think further into the concepts for a deeper understanding, or to apply their knowledge with hands-on practice for problem solving. There are many ways of using class exercises. For a small class, the teacher may simply use the exercise to engage the students in discussion and practice. For larger classes, the students can form small groups to use the class exercise as an instrument to lead to group projects. Our project developed, implemented, and disseminated 16 class exercises (Wu, Manohar, & Acharya, 2016). Each class exercise consists of the exercise description, instruction notes, student handout, and assessment instrument.

An example for discussion may be Module RM03, under Requirements Management. The learning objective is in discerning between business requirements and functional requirements. It is a communication skill too often students training in technical subjects lack. The class exercise leads the students to go through a list of requirements statements and discuss whether each one is a business requirement statement or a functional requirement statement. The students are expected to have prepared themselves studying the textbook definitions of the two different requirement statements. But even if some are not very thorough in their studying, the in class exercise tends to engage them to want to refer back to think deeper into what they have studied. A detailed evaluation of the Class Exercises is presented in Wu, Manohar and Acharya (2016). Table 2 lists all the Class Exercise Modules in the project, and they are all publicly accessible at the courseware repositories discussed in Section 6.

Case Study Videos

Teachers quite often use videos to enhance the classroom learning experience. Video in general is not interactive. It may not be considered student-centric. But video, if designed right and put together well, can be extremely engaging. The media of sight and sound together with a good narrative or story line can create an immersive experience for the viewer. Students can use video to reinforce reading and studying of lecture materials, or to understand and follow instructions watching demonstration. To an entire class, watching video together can help the class to share a common basis of knowledge and that may enhance the quality of discussion and overall student comprehension. Videos can aid in illustrating highly complex concepts and ideas in a short amount of time, provoking meaningful discussion as well as analysis (Saltrick, Honey & Pasnik, 2004). In the project, we used case study videos primarily to provide a realistic way to experience SV&V best practices in industry, even personally. Produced from the scripts first drafted by our industry partners and confirmed by the testimonies shared in focus group discussions, each case study video portrayed a realistic picture for the audience to appreciate the process of SV&V best practice. For example, the video on peer code review showed also how potential tension or conflict might arise in the human interaction. When viewing the video on requirements elicitation, the viewer might gather the tedious and detailed nature of the work and feel it more personally. Figure 3 below is a scene captured from the Case Study Video on Security Inspection. Our project produced, implemented, and disseminated 4 case study videos (Acharya, Manohar & Wu, 2017). Each case study video consists of the digital video, the video description, discussion questions, and an assessment instrument.

SV&V Area	Class Exercise	mins
Requirements Management	Ambiguous Questions	25
	Business Requirements and Functional Requirements	50
	Clarifying User Requirements	50
	Needs Statement to SRS	50
	Needs Statements to User Requirements	50
	Requirement Ambiguity	50
	Stated and Implied Requirements	25
Configuration Management	Defect Lifecycle	50
Software Reviews	Code Inspection	150
	Review a given SRS with Checklist	100
Software Testing	Cost Effective Testing Approach	50
	Test Cases for a Given Requirement	50
	Testing Tools	50
	Understanding Testing	50
Additional Topics	Deming’s 14 Points on System of Profound Knowledge (SoPK)	50
	Understanding IEEE Standards	50
	TOTAL	900
	Contact hours (in 50 min periods)	18

Table 2. Class Exercise Modules

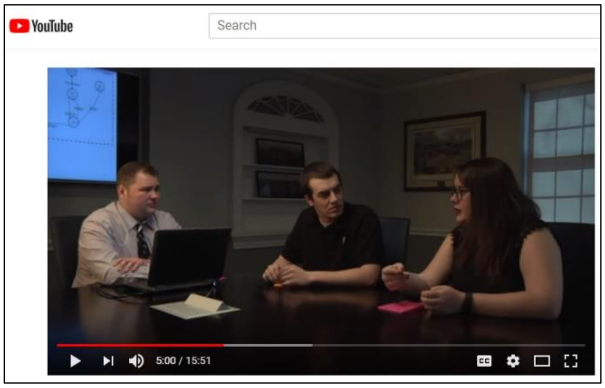


Figure 3. Security Inspection Scene

Table 4 lists all the Case Study Videos produced by the project. The videos are posted to YouTube for streaming. The hyperlinks to play the videos are accessible from the courseware repository discussed in Section 6.

SV&V Area	Case Study Video	mins	# of Scenes
Requirements Management	Requirements Elicitation	100	5
	V&V in Scrum	50	4
Software Reviews	Code Inspection	100	7
Software Testing	Testing and Security	50	5
	TOTAL	300	21
	Contact hours (in 50 min periods)	6	

Table 4. Case Study Videos

Development Methodology

The ALTs were meant to address the gaps in the SV&V curriculum identified in our critical review by the focus groups. While the authors led the development of the ALTs, we also acquired the help of the project partners to incorporate academic research and industry best practices into our effort. We started with assessing the current academic offerings as well as the industry requirements. Our gap analysis would identify the knowledge areas where the inadequacies would be addressed in the ALTs. We applied the Analysis-Design-Development-Implementation-Evaluation (ADDIE) instruction design framework to iteratively assess the course content and the delivery for further revision and improvement (Morrison, 2010). Figure 5 depicts the iterative ADDIE framework applied in our development methodology, with the key activities of review performed by our academic-industry partners in the focus groups. An English Language Editor edited the final products prior to dissemination.

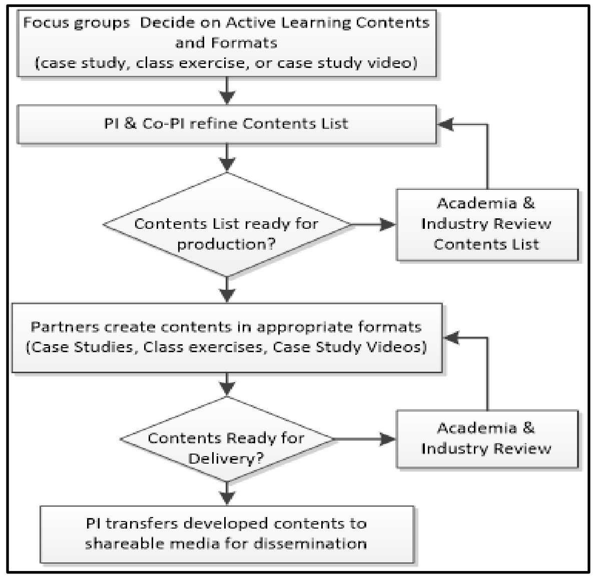


Figure 5. Applying the ADDIE framework

Using the ADDIE methodology the project team produced and disseminated the ALTs for 44 delivery contact hours of SV&V courseware. The ALTs were modularized into small modules of 25 delivery minutes each, for easy adaptability.

Delivery Model

The ALTs were designed to engage the students, to impart practical knowledge into theoretical understanding. Learning still largely depends on the students' knowledge retention. The classroom delivery of the ALTs would create the setting for the students in retention activities, such as group discussion, further studying and deeper thinking in the assignments and team projects (Mishra, Hacaloglu, & Mishra, 2014). It is important to identify and incorporate the delivery strategies to meet the learning outcomes for the ALT modules.

We used a flipped classroom model (Bonwell & Eison, 1991) which allowed us to maximize utility of the class time to engage the students and incite further activities in knowledge retention. Students were expected to be prepared prior to class time and outside the classroom. There were assigned textbook readings or reviewing of lecture materials online. For effective delivery we also recommended the students to work in small teams. Overall, the flipped classroom model has proven highly effective at increasing student engagement and enhancing the preparation of students for class sessions (Day & Foley, 2006). The flipped classroom also has been shown to allow the instructor to cover more material and results in higher student performance (Mason, Shuman & Cook, 2013).

Different ALTs engaged the students in different ways. The Case Studies were explicit in the approach: each Case Study made the point to consider issues in realistic practices. Instructors presented the Case Study while guiding students into further study and discussion of the practical issues in SV&V. The Class Exercises were designed for interaction in the classroom. The instructor would bring up the question(s) and serve as a moderator to guide the discussion. The instructor might also use the Class Exercise to lead students into subsequent group or individual projects. The "Instructor Notes" component of the Class Exercise covered some of these possibilities. The Case Study Videos, by nature as multimedia, were highly engaging. The videos shared real-life perspectives of actions and their consequences. The videos by design were in sequences of scenes. For instructional purposes, we found it highly beneficial to pause the video at appropriate moments to engage the class in discussion on the spot.

To adapt to the situations in different institutions including on-the-job training in industry, we modularized the ALTs into modules of 25 delivery minutes each. Instructors may consider the various needs of curriculum design, class size and class time to adjust their delivery strategies. Although we recommended it, the flipped classroom model is not imperative. Instructors may also choose to only adopt that partially. In summary, the following are our recommendations for the delivery strategies for the ALTs.

- Use the flipped classroom model, if applicable.
- Have students work in small teams of two or three each team.
- Deliver the ALTs in sessions of one or multiple modules.
- Apply the assessment instrument to evaluate learning outcomes immediately after each session.

5. TRAINING WORKSHOPS

During the second and third years of the project, we organized two SV&V Training Workshops to disseminate and promote the use of the developed ALTs. In the one-and-a-half day workshop, we introduced the ALTs to the attendants, shared the delivery model, and chose to demonstrate several of the ALT modules followed by feedback and discussion.

We held the workshops in the authors' institution and invited not only our implementation partners but also many other institutions and industry partners to attend. The attendants were granted access to the ALTs in our repository and everyone was provided with a complete instructor's kit. We strongly encouraged consideration to implement them in their home institutions, offering post-workshop assistance to them in many ways. We gained not only much valuable feedback, but also a much larger group of implementation partners. We went into much collaborative activities with some of the partners and were much gratified when ended up seeing lasting changes in the curriculum and course contents in the partner institutions.

	Institutions shared the ALTs with
1	Auburn University, AL
2	Baldwin Wallace University, OH
3	Bowie State University, MD
4	Clarion University, PA
5	East Carolina University, NC
6	Eastern Mediterranean University, Cyprus
7	Embry-Riddle Aeronautical University, FL
8	Fairfield University, CT
9	Faulkner University, AL
10	George Mason University, VA
11	Georgia Southern University, GA
12	Grand Valley State University, MI
13	Indiana University Southeast, IA
14	Kennesaw State University, GA
15	Kentucky State University, KY
16	Kenyon College, OH
17	Milwaukee School of Engineering, WI
18	Minnesota State University, MN
19	Montana Tech, MT
20	Mount Mercy University, IA
21	North Carolina A&T State University, NC
22	Northwest University, South Africa
23	ORT Braude College, Israel
24	Rocky Mountain College, MN
25	Rose-Hulman, IN
26	SUNY Oneonta, NY
27	University of Alaska Southeast, AK
18	University of Maryland, MD
29	University of Michigan-Dearborn, MI
30	University of South Carolina Upstate, SC
31	Virginia State University, VA
32	Whitworth University, WA

Table 6. Shared ALTs with these Universities

The two training workshops were held in August, of 2015 and 2016. Other abridged versions of the workshop were also held in the following years at some other conferences. Table 6 above lists the institutions we shared the ALTs with, and 20 of these institutions attended at least one of the two training workshops. We offer the information to share the level of our effort toward meeting the broader impacts requirements of an NSF funded project.

6. COURSEWARE REPOSITORY

We initially used the Dropbox as the central repository to share the courseware products, i.e., the ALTs. Now the ALTs are made available for public access on the web. There are two web portals. One is the project web site administered by the authors' institution (www.rmu.edu/nsfvv). The home page is depicted in Figure 7. The other is the web portal to connect computing educators administered by Ensemble, a pathway project funded by National Science Foundation for the National Science Digital Library of computing education resources (www.computingportal.org / softwareverficiationvalidation). Figure 8 depicts the web portal at Ensemble.

Figure 7. Repository home page at project web site

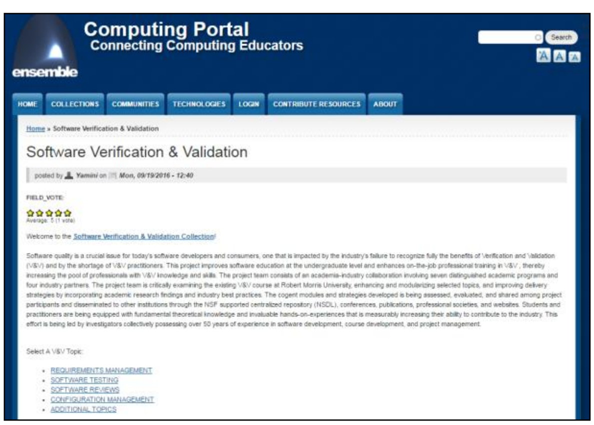


Figure 8. Repository web portal at Ensemble

At the web portals, the ALTs and the supporting documents are organized by the SV&V topic each pertains to. The topics are: Requirements Management, Software Reviews, Configuration Management, Software Testing, and an Additional Topics. Underneath each topic, there are the 3 categories of the ALTs: Case Studies, Class Exercises, Case Study Videos. The ALTs are kept there and available for download, except for the Case Study Videos. The videos are posted to YouTube for streaming, accessible via a hyperlink to play. Figure 3 above shows a scene of a Case Study Video streaming on YouTube.

7. INTELLECTUAL MERIT

The project team developed, tested, implemented and disseminated 31 ALT modules for 44 delivery contact hours over the project duration as described in sections 3, 4, 5 & 6. These ALTs can be readily incorporated in existing SE, CS, IS and CE curricula partially or in its entirety. In the case of a new course in SV&V, it was incorporated entirely. The research findings regarding the effectiveness of the ALTs have been disseminated through conferences and journal publications. To date, the research results have been presented at ASEE 2014, ASEE 2015, EDSIGCON 2015, ASEE 2016, WMSCI 2016, ASEE 2017 and ASEE 2018 annual conferences. A keynote address on Software Verification and Validation was delivered in WMSCI 2016. In 2016 this project was presented at the NSF Showcase at SIGCSE 2016 and in the Envisioning the Future of Undergraduate STEM Education: Research and Practice symposium organized by AAAS in 2016. In the duration of the project from 2014 to 2018, twelve conference papers and seven journal papers were published. A book on SV&V Case Studies has been published by the Alexandria Street Press (online), and a workshop using the ALTs was conducted in EDSIGCON 2016.

8. BROADER IMPACT

Originally the project proposed to disseminate the developed ALTs to ten other institutions. As of date the ALTs have been shared among all project partners and disseminated to 30 US institutions and 3 international institutions as described in sections 5 & 6. The dissemination took place through training workshops, scholarly research publications as well as sharing of tools on the web. Two websites serve as repository for the project deliverables: the NSF-funded Ensemble repository and our own hosting institution, supported with streaming via YouTube. The ALTs are also readily usable for on-the-job training in industry. The project generated SV&V awareness and planted the growth of competent SV&V practitioners. Beyond the enhanced SV&V course itself, this project contributed to the development of a SV&V community spanning industry and academia.

9. SUMMARY

We reported on the effort of our NSF funded project in the TUES program to transform undergraduate education in STEM. Motivated by the scarcity of SV&V practice in the software industry even when it was proven to be effective to ensure software quality. We brought in the support of collaborative partnership of academia as well as industry. The partnership formed focus groups to critically review the existing SV&V curriculum. We then proceeded to develop new Active Learning Tools (ALTs) for a new teaching approach for SV&V. The focus groups helped to refine the ALTs through iterative re-development. The ALTs introduced a new pedagogy. Through training workshops to share and promote the ALTs, we also gained feedback to improve them and our delivery strategies as well. Since we invited more to join the workshops, we broadened the partnership to deploy the new ALTs. In some cases we began to observe lasting changes in their SV&V curriculum and course contents. The continued dissemination of the new pedagogy we hope will result in more intellectual merit, broader impact and build a sustained community skilled in SV&V.

10. ACKNOWLEDGEMENTS

The project was supported by National Science Foundation through the NSF-TUES Award, Grant# 1245036. The authors gratefully acknowledge this support. We also want to express our deepest appreciation to all our project partners, in academia and in industry, for their enthusiastic support and collaboration. It was a most rewarding learning experience for us.

11. REFERENCES

Acharya, S., P.A. Manohar, & P. Wu (2017) Using Case Study Videos as an Effective Active Learning Tool to Teach Software Development Best Practices, *Journal of Systemics, Cybernetics & Informatics 15*(3), 70-75. ISSN#1690-4524.

Arthur, J.D., M.K. Groener, K.J. Hayhurst, & C.M. Holoway (1999). Evaluating the Effectiveness of Independent Verification and Validation. *IEEE Computer 32*(10), 79-83.

Arthur, J.D., R.E. Nance, J.A. Joines, R.R. Barton, K. Kang, & P.A. Fishwick (2000). Verification and Validation without Independence: a Recipe for Failure. Proceedings of the 2000 Winter Simulation Conference, pp.859-865.

Bonwell, C.C., & J.A. Eison (1991). Active Learning: Creating Excitement in The Classroom. *ASHE-ERIC Higher Education Report No.1*. The George Washington University, School of Education and Human Development. Washington, D.C. Retrieved from http://files.eric.ed.gov/fulltext/ED336049.pdf

Davis, C. & E. Wilcock (2003). *Teaching Materials Using Case Studies*. UK Centre for Materials Education.

Day, J.A., & J.D. Foley (2006). Evaluating a Web Lecture Intervention in a Human–Computer Interaction Course. *IEEE Transactions on Education 49*(4), 420–431.

Frydenberg, M. (2013). Flipping Excel. *Information Systems Education Journal 11*(1) 63–73. ISSN#1545-679X.

Grant, R. (1997). A Claim for The Case Method in The Teaching of Geography. *Journal of Geography in Higher Education 21*(2), 171–185.

IEEE/ACM (2014). Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering. *IEEE/ACM Software Engineering 2014.* The Computing Curricula Series, by the Joint Task Force on Computing Curricula of IEEE Computer Society and Association of Computing Machinery. Feb 23, 2015.

Manohar, P.A., S. Acharya, P. Wu, M. Hansen, A. Ansari, & W. Schilling (2015). Case Studies for Enhancing Student Engagement and Active Learning in Software V&V Education. *Journal of Education and Learning 4*(4), 39-52. ISSN#1927-5250.

Mason, G.S., T.R. Shuman, & K.E. Cook (2013). Comparing the Effectiveness of an Inverted Classroom to a Traditional Classroom in an Upper-Division Engineering Course. *IEEE Transactions on Education 56*(4), 430,435.

Mishra, D., T. Hacaloglu, & A. Mishra (2014). Teaching Software Verification and Validation Course: A Case Study. *International Journal of Engineering Education 30*(6A), 1476-1485.

Morrison, G.R. (2010). *Designing Effective Instruction* (6*th* edition). John Wiley & Sons.

Pham, H. (1999). Software Reliability. John Wiley & Sons, Inc. p. 567. ISBN#981308384.

Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education, 93*(3), 223–231.

Raju, P.K., & C.S. Sanker. (1999). Teaching Real-World Issues Through Case Studies. *Journal of Engineering Education 88*(4), pp. 501–508.

Saltrick, S., M. Honey, & S. Pasnik (2004). Television Goes to School: The Impact of Video on Student Learning in Formal Education. Center for Children & Technology, Education Department, Corporation for Public Broadcasting.

Sivan, A., L.R. Wong, C. Woon, & D. Kembler. (2001). An Implementation of Active Learning and Its Effects on The Quality of Student Learning. *Journal of Innovations in Education and Training International 37*(4), 381–389.

Wang, C-W., J.S. Ostroff, & S. Hudon (2014). Precise Documentation and Validation of Requirements. *Formal Techniques for Safety-Critical Systems*. (Artho & Olveczky, eds). Springer. ISBN#9783319054162.

Woods, D., & E. Howard (2014). An Active Learning Activity for an IT Ethics Course. *Information Systems Education Journal 12*(1) 73–77. ISSN#1545-679X.

Wu, P., P.A. Manohar, & S. Acharya (2016). The Design and Evaluation of Class Exercises for Active Learning in Software Verification and Validation. *Information Systems Education Journal 14*(4), 4–12. ISSN#1545-679X.

Data Cleansing: An Omission from Data Analytics Coursework

Johnny Snyder
josnyder@coloradomesa.edu
Business Department
Colorado Mesa University
Grand Junction, CO 81501

Abstract

Quantitative decision making (management science, business statistics) textbooks rarely address data cleansing issues, rather, these textbooks come with neat, clean, well-formatted data sets for the student to perform analysis on. However, with a majority of the data analyst's time spent on gathering, cleaning, and pre-conditioning data, students need to be trained on what to look for when generating or receiving data. A critical scan of the data needs to be performed (at a minimum) to look for errors in the data set before data analysis can be performed.

Keywords: Data cleansing, data pre-conditioning, data analysis, data formatting, Pareto Principle

1. INTRODUCTION

Data gathering and cleansing is the first task an analyst must perform before analytical tools can be applied to the data. Data issues such as non-printing characters, misspellings, text embedded in the quantitative data, interpretation, imputation, or unit conversions all must be accomplished before the data is ready for analysis.

In this, the information age, new positions in corporate structures call for positions such as "data steward" and "data analyst" who, among other things are responsible for:

- extracting existing data
- performing data validation
- confirming data correctness
- confirming data upload
- identifying data quality issues
- identifying and analyze defects in data sources and processes
- receiving, inspecting, validating, transforming, cleaning, and loading data received in a variety of formats (Monster, 2018).

These responsibilities illustrate that the corporate data person spends most of their time managing data rather than analyzing data. Ruiz (2017), while dubbing data science as "the sexiest job of the 21st century," also noted that "most data scientists spend only 20% of their time on actual data analysis" (para 1). These data cleansing items that a data analyst must be (primarily) responsible for consume a large part of their day, so merit inclusion in the quantitative methods classroom.

The 80/20 Rule (aka the Pareto Principle) appears in many situations in business and other human activities (Koch, 1998). There are many examples of the 80/20 rule online, in the academic literature, and in books such as Koch (1998). The definition of the Pareto Principle is simple, "a prediction that 80% of the effects come from 20% of the causes" (Mar, 2013, para. 4).

Many people have used the Pareto Principle in business, in computer coding, in describing computer trouble shooting activities, in product management, and in organizing one's personal life activities! One recent application of the 80/20 rule can be useful to new job titles such as: data steward, data analyst, business analyst, data scientist…of the information age, or the age of big data. This rule is stated as: 80% of a data scientist's time is spent collecting, organizing, and cleansing the data, while only 20% of the time is spent analyzing the data.

However, this rule of thumb is not being taught in many quantitative methods textbooks. The data sets a student sees in these classes are neat, clean, organized, and ready for analysis – not quite the way data generally comes to an analyst in its native form.

This case illustrates that data is messy, full of human errors or misinterpretations, incorrect, misspelled, illegible, or incorrectly formatted; thus, in need of pre-conditioning (cleansing) before analysis can begin.

2. LITERATURE REVIEW

Data cleaning has traditionally been a "lower status" of data quality activities, bordering on data manipulation (Van den Broeck, Cunninghan, Eeckels, & Herbst, 2005). Part of this reputation could be due to the prevalence of how data errors can be "fixed." For example, missing data values can be addressed by:

- deletion – exclude the instance
- hot deck – replace using values from the same data set
- imputation – assign a representative value (mean, median) to a missing one (Corrales, Corrales, & Ledezma, 2018)

How one does data cleansing is still a topic open to debate, and might have factors such as type of data, application for data, source of data, and discipline specific conventions to consider when making data cleansing decisions. However, it has been observed that students are not well trained in the methods of data preparation (for analysis) but seem to be able to come up to speed rather rapidly (Yue, 2012).

In the 20th century, the 80/20 Rule was shown to describe library usage patterns – 20% of the patrons use 80% of the resources (Trueswell, 1969), posting to electronic bulletin boards – 20% of the participants post 80% of the content (Echavarria, Mitchell, Newsome, Peters, & Wentz, 1995), consumer spending patterns – 20% of the customers account for 80% of the revenue (Fitzsimmons, 1985), and of course, Pareto's original assertion that 20% of the population of a country owns 80% of the land (Pareto, 1971).

More recently, in the 21st century, the 80/20 rule has been observed in computer code – 20% of the code contains 80% of the errors (Pressman, 2010), healthcare – 20% of the patients use 80% of healthcare services (Weinberg, 2009), and 80% of the defects can be explained by 20% of the causes in a quality control environment (the famous Pareto Chart) (Larson, 2018).

In the case of business analytics, or the study of data and what information can be gained from the data, the 80/20 rule becomes: 80% of the time spent by a data scientist is on gathering, cleansing, and storing the data, while 20% of the time is spent on analyzing the data. However, this concept is not discussed in most quantitative methods textbooks, thus, students enter the workforce with unrealistic expectations of how data will be coming to them. For example, Render, Stair, Hanna, and Hale (2018) state: "…collecting accurate data can be one of the most difficult steps in performing quantitative analysis" (p. 4). This is a true statement, and methods for collecting data are then presented, but there is no mention of cleansing data, or examples of data needing cleansing presented. Groebner, Shannon and Fry (2014) discuss how to collect data (surveys, observation, personal interviews), collection issues (bias, accuracy, error), and sampling techniques, but no mention of data cleansing or examples or problems/exercises are presented.

The literature regarding data cleansing includes the ETL (extraction, transformation, and loading) process for a database or data warehouse (Boyno, 2003), data quality in regression models (Corrales, Corrales, & Ledezma, 2018), as well as harvesting, cleaning and analyzing Twitter data (Hill & Scott, 2017).

These papers point to what Hellerstein (2008) infers when he states: "Data collection has become a ubiquitous function of large organizations – not only for record keeping, but to support a variety of data analysis tasks that are critical to the organizational mission" (p. 1). In short, business has become data driven, and as the old acronym tells us: GIGO. Keeping the data accurate, formatted correctly, and timely has become a new job in corporations – that of the data scientist or data steward (Experian, 2018). These "newer" positions in the corporate structure illustrate the importance of obtaining, storing, and utilizing data in business decision-making processes. As Hellerstein (2008) states: "Data errors can creep in at every step of the process from initial data acquisition to archival storage" (p. 1).

Data collection and cleansing is the first step of the analysis process and must be taken seriously (GIGO). Preparing data for analysis is critical if good information is to be extracted from data flows. The first steps are illustrated in this paper, where data is collected, cleansed, and prepared for simple analysis. Many further activities for data cleansing are context dependent as illustrated previously in the literature review. However, the steps illustrated in this case are universal and should be performed on any data set an analyst receives.

3. METHOD

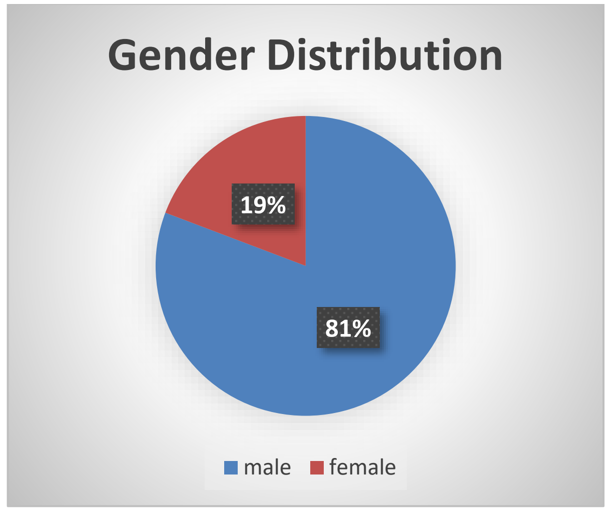
A survey instrument was created to gather student data from an introduction to business analysis class (see Appendix A). This instrument contains questions intended to solicit answers from all data categories (Nominal, Ordinal, Interval, Ratio - NOIR) to aid further classroom discussions about data types and graphical and analytical techniques associated with them. The survey is anonymous and is distributed on the first day of class. The instructor collects the survey instrument and inputs the data into an Excel (Excel, 2016) spreadsheet and distributes the spreadsheet to the class. (See Appendix B) The resulting spreadsheet is used to discuss (throughout the class) data types (NOIR), data errors (units missing), different units from different survey respondents, interpreting what the survey respondent "meant", text characters input into Excel cells (Excel refuses to do analysis on these cells), data conversions (from feet/inches to inches for example), and the dreaded non-printing character (space, for example) which can foul up the simplest Excel operations.

4. RESULTS

One of the first exercises for students could be to graph a nominal variable such as gender which is easy due to the pre-defined selection on the survey instrument. Manipulating the data into a form ready to graph, we obtain Table 1. Note for students: be sure to track n, the sample size, to be sure all data values have been accounted for. It should also be mentioned that this is one of the only "clean" parts of the data set…one of the columns that are ready for analysis!

Gender	Frequency	Percent
male	21	0.807692308
female	5	0.192307692
n =	26	1

Table 1 - Gender



Graph 1
Gender Distribution

The next exercise could be to evaluate the students' favorite color or type of security software they use. Analyzing these, using a pie chart or bar chart (or a Pareto Chart), would be straight forward if the data were clean, but looking at Appendix B, the results from the survey are not ready for analysis.

Attempting to organize the favorite color column results in questions about the data that must be addressed before a frequency distribution can be constructed. Some of these questions include:

- Is maroon brown or red or its own color?
- What color is blue/black? (counting both would artificially increase n)
- Should navy blue be counted as blue?

After a first pass at constructing a frequency distribution, depending on the Excel count function utilized, it could be found that n = 24 instead of 26. This is an interesting result for students, as the difference is due to colors being entered with a space (a non-printing character) at the end (or beginning) of the cell, resulting in Excel not counting these data points. Once these two cells have been identified and cleansed, the resulting frequency distribution can be seen in the third column of Table 2.

Non-printing characters can give the data analyst a lot of grief! Space is the most common non-printing character, but many others exist, such as carriage return (enter), end of record and end of file characters from various software packages that the analyst might have to import into their computing environment.

Upon cleansing the data, the color black was removed from the distribution (blue/black was cleansed to blue, the respondents first color choice). In a practical application, such as scheduling the percentage of cars to paint of each color for the coming model year, this cleansing activity can have the consequence of removing a very popular color from a dealer's inventory. Thus, the analyst needs to consider the business need for the data before cleansing the data.

Color	Frequency (original)	Frequency (cleansed)
blue	10	11
red	4	4
green	3	3
purple	2	2
white	1	1
orange	1	1
maroon	1	1
yellow	1	1
grey	0	1
gold	1	1
n =	24	26

Table 2
Favorite Color

Here are a couple of rules to follow when cleansing a data set:

- Maintain an original copy of the data.
- Label all pre-conditioning or cleansing activities (i.e. tell the reader what you have done to the data).
- Discuss the cleansing activities with your team to be sure that the business consequences for data cleansing have been addressed.

A fun exercise is to compute the average height of a student in the class. This is a seemingly straight-forward calculation, but if you ask Excel to compute the average from the data as it stands, it yields a #DIV/0! error. The original data and the cleansed data are shown in Table 3, where the cleansed data has been converted to a numerical value (from feet and inches) for Excel computations, units have been added in the heading, and the average has been computed.

	Height (original)	Height (inches) (cleansed)
	6'1" 73"	73
	6'4"	76
	5'11"	71
	6'2"	74
	5'7"	67
	5'9"	69
	5'8"	68
	5'7"	67
	5'11"	71
	6'4"	76
	6'3"	75
	6'0"	72
	5'5	65
	5'11"	71
	5'4"	64
	5'11"	71
	6'5"	77
	6'0"	72
	5'4"	64
	5'11	71
	5'6	66
	6'3"	75
	6'2	74
	6'5"	77
	5'8"	68
	5'10"	70
Average	#DIV/0!	70.92308
n =	26	26

Table 3
Height

Note also that upon cleansing the data, one should add the data units to the column heading for clarification purposes. Students also need to be careful when converting from the original to the cleansed form, as this is a manual operation, and errors can arise! Every time a human "touches" the data, errors can enter into the data set.

Another seemingly straight-forward calculation is to compute the average shoe size of a person in the data set. One could even compute the average size by gender, which makes more sense from a retail perspective. The sorted data is shown in Table 4.

	Gender (m/f)	Shoe Size (original)	Shoe Size (US size) (cleansed)
	f	8.5	8.5
	f	9	9
	f		
	f	7.5	7.5
	f	10	10
	m	12	12
	m	12	12
	m	9	9
	m		
	m		
	m		
	m		
	m	10 in	10
	m	12	12
	m	9	9
	m	11.5	11.5
	m	10 1/2	10.5
	m	10	10
	m	13	13
	m	11	11
	m	10.5-11	10.75
	m	12	12
	m	13	13
	m	12	12
	m	10.5	10.5
	m	11	11
n =	26	21	21

Table 4
Shoe Size

Table 4 illustrates for the student other issues that come with open ended survey questions. While 10 ½ is a valid shoe size, 10.5 is more appropriate for computational purposes (Excel readability – i.e. no text characters). Other questions can arise as well, such as:

- Should 10.5-11 be recorded as 10.75, the arithmetic average? or 10.5? or 11?
- What should we do about missing values?
- What does 10 in mean as a shoe size?

Finally, keep the units in the header row, not associated with the individual data values, again for computational purposes, because this is how Excel requires data to be formatted.

Many other ideas and examples can be created from a small data set such as this one, which illustrates for the students how easily data flows can be contaminated, inadvertently, by humans, machines, or software.

5. CONCLUSIONS

In coursework covering quantitative methods, spreadsheets or data sets come to the student pre-conditioned, or cleansed, ready for analysis. However, in business applications, the data might come in to the analyst in a raw form and need to be cleansed. Some of the issues that should be addressed include:

- units and unit conversions
- missing values
- extra text characters
- unclear answers (survey responses)
- non-printing characters

This case illustrated a simple but effective method to show students some of the issues that arise with data cleansing and how to address these issues in order to obtain a data set ready for analysis. Further, this data set can be used to explore different data types (NOIR), graphical representations of the various data types, and many concepts in data analysis from descriptive statistics to hypothesis testing…once the data is cleansed!

6. REFERENCES

Boyno, E. (2003). Extraction, transformation, and loading in a data warehouse course. Information Systems Education Journal 1(10). p. 3-10.

Corrales, D., Corrales, J., and Ledezma, A. (2018). How to address the data quality issues in regression models: a guided process for data cleaning. Symmetry 10(99). p. 1-20.

Echavarria, T., Mitchell, B., Newsome, K., Peters, T., and Wentz, D. (1995). Encouraging research through electronic mentoring: A case study. College and Research Libraries, 56 (4): 352-361. doi: 10.5860/crl_56_04_352

Excel. (2016). Computer software. Redmond, WA: Microsoft.

Experian. (2018). Data Steward. Retrieved from: https://www.edq.com/uk/glossary/data-steward/

Fitzsimmons, J. (1985). Consumer Participation and Productivity in Service Operations. Interfaces, 15(3), p. 1-146.

Groebner, D., Shannon, P., and Fry, P. (2014). Business Statistics: A Decision Making Approach (9th edition). Boston, Mass: Pearson.

Hellerstein, J. (2008). Quantitative data cleaning for large databases. Retrieved from: http://db.cs.berkeley.edu/jmh/papers/cleaning-unece.pdf

Hill, S. and Scott, R. (2017). Developing an approach to harvesting, cleaning, and analyzing data from Twitter using R. Information Systems Education Journal 15(3). p. 42-54.

Koch, R. (1998). The 80/20 Principle: The Secret to Achieving More with Less. New York: Doubleday.

Larson, (2018). Using the 80/20 Rule to Improve Quality in Auto and Aerospace Manufacturing. Retrieved from: https://www.beaconquality.com/blog/using-the-80/20-rule-to-improve-quality-in-auto-and-aerospace-manufacturing

Mar, A. (2013, May 31). 13 examples of the Pareto Principle. Retrieved from: https://management.simplicable.com/management/new/examples-of-the-pareto-principle

Monster (2018). Data steward jobs. Retrieved from: https://www.monster.com/jobs/search?q=data-steward&jobid=2bc7ea0b-0fcb-4aa1-a026-db37660cb157

Pareto, V. (1971), Translation of Manuale di economia politica (Manual of political economy), Page, A.

Pressman, R. (2010). Software Engineering: A Practitioner's Approach (7th ed.). Boston, Mass: McGraw-Hill.

Render, B., Stair, R., Hanna, M., and Hale, T. (2018). Quantitative Analysis for Management (13th edition). Boston, Mass: Pearson.

Ruiz, A. (2017, Sept. 26). The 80/20 data science dilemma. Retrieved from: https://www.infoworld.com/article/3228245/data-science/the-80-20-data-science-dilemma.html

Trueswell, R. (1969). Some behavioral patterns of library users: The 80/20 Rule. Wilson Libr Bull, 43(5), p. 458-461.

Van den Broeck, J., Cunningham, S., Eeckels, R. and Herbst, K. (2005). Data cleaning: detecting, diagnosing, and editing data abnormalities. PLoS Med 2(10).

Weinberg, M. (2009, July 27). In health-care reform, the 20-80 solution. Retrieved from: http://www.projo.com/opinion/contributors/content/CT_weinberg27_07-27-09_HQF0P1E_v15.3f89889.html

Yue, K. (2012). A realistic data cleansing and preparation project. Journal of Information Systems Education, 23(2). p. 205-21

Appendix A – Data gathering survey

Class Survey – first data set!

Demographic Information
Gender: □ Male □ Female Year of birth:
Height: Shoe Size:
Number of: Brothers _________ Sisters _________ - you have
Favorite color: ________________________
I am looking forward to this class: (circle on the next line)
Strongly agree = 1 2 3 4 5 = Strongly disagree
Type of PC Security Software you use: ________________________
Major area of study:

Appendix B – The data set….as respondents answered

Class Data										
Survey Number	Gender	Year of Birth	Height	Shoe Size	Brothers	Sisters	Favorite Color	Looking Forward	Security Software	Major Area of Study
1	m	1997	6'1" 73"	12	0	1	red	4	microsoft windows	marketing
2	m	1998	6'4"	12	0	1	maroon	3	slim cleaner +	accounting
3	m	1997	5'11"	9	1	1	green	3	?	business
4	m	1998	6'2"		1	1	blue/black	2	norton safe security	business admin
5	m	1997	5'7"		0	2	blue/black	2	?	accounting
6	m	1998	5'9"		1	1	blue	3	none	business
7	m	1997	5'8"		4	2	yellow	2	none (self watched)	cis
8	f	1997	5'7"	8.5	1	2	purple	3	don't know	accounting
9	m	1995	5'11"	10 in	6	0	navy blue	3	Macfee	management
10	m	1997	6'4"	12	0	1	gold	2	Microsoft	finance
11	m	1997	6'3"	9	2	0	grey	2	mac	management
12	m	1997	6'0"	11.5	0	2	green	3	Norton	marketing
13	f	1996	5'5	9	1	0	green	3	I don't know	accounting
14	m	1996	5'11"	10 1/2	1	3	blue	2	none	economics
15	f	1999	5'4"		0	1	red	2	McAfee	accounting
16	m	1979	5'11"	10	0	1	blue	2	Mac	cis
17	m	1998	6'5"	13	1	0	blue	1	Apple	management
18	m	1997	6'0"	11	1	0	orange	3		management
19	f	1997	5'4"	7.5	0	1	blue	2	Mac	culnary arts/hospitality management
20	m	1998	5'11	10.5-11	1	4	blue	4	McAfee	marketing
21	f	1998	5'6	10	1	2	red	3	McAfee	cis
22	m	1998	6'3"	12	1	0	red	2	Mcafee	entreprenuership
23	m	4/22/1998	6'2	13	1	1	white	3	none	business
24	m	1998	6'5"	12	2	1	blue	3	Microsoft	finance
25	m	1996	5'8"	10.5	1	3	purple	4	Microsoft	administration
26	m	1996	5'10"	11	0	1	blue	2	Norton, Homebuilt	cis

Process-Focused Approach to a Systems Analysis & Design Group Project

Aditi Mukherjee
aditmukherjee@ufl.edu
Information Systems and Operations Management

Sarah Bleakney
Sarah.bleakney@warrrington.ufl.edu
Teaching and Learning Center

University of Florida
Gainesville, FL 32611

Abstract

This case study describes an alternative process-focused approach to a group project assignment in an undergraduate Systems Analysis and Design (SAD) course. This approach more closely reflects the incremental and iterative nature of Information Systems Development Projects (ISDP) through expanded scope, modified instructions, and reallocation of class time. This approach enables students to select their own real-world ISDP and apply a wider breadth of course concepts in that context, while gaining experience in critical thinking and decision making within a group setting.

Keywords: Systems Analysis and Design, group project based learning, process-focused project

1. INTRODUCTION

This case study explores a process-focused approach to the group project assignment in a half-semester long undergraduate Systems Analysis and Design (SAD) course. Group projects are a critical component of most SAD courses as they are typically used to reinforce the concepts of SAD tools and techniques via a simulated Information Systems Development Project (ISDP). These projects enable students to apply their understanding of how the tools and concepts that are being taught in lectures can be applied within the context of the ISDP. We present an alternative, process-focused approach to SAD course group projects where the pedagogical purpose of the project is shifted from solely focusing on the quality of deliverables created by students, to meaningfully conveying to them the process used to develop those deliverables.

Project-based learning (PBL) involves assigning projects that require collaboration among group members, are long-term (i.e., span the entire course), and result in students' completion of project components and a final report. (Thompson & Beak, 2007) While these projects are unable to simulate every aspect of a real-world ISDP, group PBL is a widely used pedagogy in Information Systems (IS) classes, especially for SAD. (Harris, 2007; Melin, et al., 2006; Russell, et al., 2014; Woods & Howard, 2014) Instructors often positively perceive collaborative learning experiences as opportunities to increase student motivation, performance, engagement, and autonomy of their own learning. (Lage et al., 2010; Opdecam et al., 2014; Lumpkin et al., 2015; Stefanou, et al., 2013) As a result of the collaborative problem solving and critical thinking that comes with completing projects, and the real-life context used for them, students are able to develop a variety of technical and soft (i.e., teamwork and communication) skills. (Woodward, et al., 2009; Tsay & Brady, 2010)

While group PBL offers myriad benefits, it can also be associated with a variety of limitations that can make them inadequate teaching tools. While implementation of SAD group projects can vary, they typically entail few deliverables (often just one project report) and infrequent feedback from the instructor, and may require students to work in groups outside of class. These limitations may be amplified in module classes where students have to complete projects within a very restricted time frame. These features rarely allow students to fully appreciate the iterative nature of developing an ISDP or improve on their project as the semester progresses (i.e., they just get one attempt). This approach to group projects can also often lead to ineffective collaboration between students, as they report challenges in managing interpersonal issues and finding time to meet outside the classroom. These challenges can make student group projects highly ineffective, and in turn, highly unpopular with students and instructors, despite their pedagogical importance. (Favor & Harvey, 2016)

We believe that the most significant drawback of such group projects is the overriding focus on the outcome or the quality of either the deliverables or the project reports, rather than on the process used to create the various deliverables that comprise an ISDP. This focus means that students do not have the opportunity to define or experience processes that lead to high-quality deliverables. Insufficient research exists about process-based learning, particularly within the context of SAD. In teaching SAD, we seek to covey how to design and develop information systems that support various business processes. (Fuller et al., 2010; Dennis et al., 2015) What we do not focus on enough is conveying to students the process of developing information systems.

Some of these drawbacks may be overcome through innovative approaches such as group projects that span multiple courses (such as the threaded live case studies approach described by Waguespeck, 1997), or by involving external companies as live clients. This paper aims to contribute to this list by providing an approach that can be used in shorter, time-constrained classes. This case study describes how the group project of a SAD class can be redesigned with only a few modifications to shift the focus from the end deliverable to the actual process of working on an ISDP. This approach reduces the focus on the context of the project and shifts it to the process of developing well-thought-out requirements, models, and designs for an ISDP that require critical thinking and group decision making. The purpose of this project is not just to challenge students to create high-quality deliverables, but to convey to them the details of the process of iteratively working on an ISDP.

In the following sections, we describe our approach used to transform a deliverable-oriented group project into a process-focused in-class group project in a SAD course. The goal of this course is for students to develop an understanding of both process-oriented and object-oriented tools for SAD. Enrollment of this course is capped at 45 and is intended for juniors and seniors in the undergraduate Information Systems and Operations Management major of a large public university. The course has a total of 12 two-hour class meetings over approximately six weeks.

2. DESIGN OF THE PROCESS-FOCUSED SYSTEMS ANALYSIS AND DESIGN GROUP PROJECT

Table 1. Outcome-Focused Group Project Structure

Class Meeting	Project Deliverables
3	GP#1:Member Names & Idea
4	GP#2:Proposal
7	GP#3:Requirements & DFD
10	GP#4:Functional Model
11	GP#5:Data Model
12	GP#6:Final Report & Presentation

In this section, we describe how an outcome-focused SAD group project was transformed into a process-focused group project. The outcome-focused SAD group project structure requires students to work in groups to apply the skills they learn in the class within the context of an ISDP of their or their instructor's choosing. The requirements of these projects can vary from a single project report that is submitted at the end of the course or several intermittent deliverables culminating in a final project report accompanied by a presentation (see Table 1). Originally, students collaborated with their groups on these deliverables outside of class. The instructor provided feedback on the intermittent deliverables and final project report and presentation.

The goal of this approach is for students to demonstrate their ability to create key SAD deliverables in the context of an ISDP. In contrast, with the process-focused group project, the goal is to encourage students to work in groups to research and discover possible alternatives using the appropriate techniques for each deliverable, make a collective decision, and then convey this decision using SAD tools and models. This approach has the distinct advantage of enabling students to develop and demonstrate critical thinking skills and group decision making.

In order to achieve this goal, the execution of the project incorporated three major changes. The first change was to increase the number of deliverables. This allowed the students to work incrementally on the project without being overwhelmed by its vast scope. This change also facilitated frequent feedback and iterative development, which reflects the nature of ISDP. The second change was to frame the requirements of the deliverables in a way that guided students through group thought processes and decision making. The instructions provided to students described the requirements of each deliverable, supported with guided prompts. The third change was to allocate in-class time for students to work on the group project. This allowed the instructor to act as mentor while students worked on the project by answering questions, clarifying the process, and guiding decision making when necessary.

We discuss each of these changes in more detail below.

Daily Project Deliverables

With the process-focused approach, students work in groups to submit one deliverable for each class meeting. Each deliverable (as outlined in Table 2) corresponds to a sequential activity in the systems development life cycle (SDLC) and builds on the previous one, which means that students work on a large project in an incremental fashion throughout the course, reflecting a real ISDP. This increase in deliverables provides a pedagogical benefit as students experience the same ISDP in greater depth and from varying perspectives (six models compared to three models in the previously used outcome-focused approach). As a result, the redesigned group project covers more course concepts than the outcome-focused approach, providing students with a more complete picture of the ISDP.

Table 2. Process-Focused Group Project Structure

Class Meeting	Project Deliverables
1	Choose Group Topic
2	GP#1:Group Introduction
3	GP#2:Project Plan
4	GP#3:System Abstract
5	GP#4:Requirements
6	GP#5:Process Model
7	GP#6:Class Diagram
8	GP#7:Use Cases
9	GP#8:Sequence Diagram
10	GP#9:Data Model
11	GP#10:Deployment Strategy
12	Final Report & Presentation

Students receive feedback on each submission within 24 hours that they can then use to revise or correct issues before they are graded on the final project report, allowing them to experience the iterative nature of ISDP. Because the project is divided into manageable components and each class is associated with one component, the instructor can intervene in a timely manner to provide guidance, coaching, and conflict resolution as appropriate. This short feedback loop enables more comprehensive and timely written and oral feedback, ensuring that students are able to incorporate any necessary changes into their next deliverable. This approach also provides students the opportunity to discuss this feedback during the next class meeting if they need additional clarification. The course grading scheme (details provided in Appendix C) used for the final report and presentation incentivizes students to carefully consider and incorporate instructor feedback.

Rewording Project Descriptions

With the process-focused approach, project descriptions were revised to include guided prompts on the process needed to complete the deliverable. The project descriptions outline those parts of each submission that students can work on individually, along with guidance on how to combine or reconcile different opinions into a single group submission. See Appendix D for an example. The descriptions are more detailed at the beginning of the semester to set up the expectations and format of the project. As the semester progresses, the instructions become less detailed as students develop skills in working cohesively as a group rather than working individually on different parts of the project. These descriptions are used to guide students through the process of developing each deliverable. Thus, the focus shifts from students being challenged to produce a deliverable to spending time on the group discussion and decision-making necessary to create the deliverable. While these in-class interactions cannot be documented or evaluated, the instructor observes the groups as they work to create the deliverables to ensure that the recommended processes are being followed.

As the groups work within a tight schedule of 40-50 minutes in class, they are provided with a resource page for each deliverable that includes detailed instructions for:

- Submission templates and guidelines
- Time-management guidelines
- Items to prepare for the next class
- Reflection prompts for the final project
-

These templates include pre-formatted submission documents, as well as symbols to be used when drawing the model diagrams. This enables students to focus on group discussion and decision making, rather than on formatting diagrams and reports.

In-Class Guidance

As detailed in Table 2, the group project consists of 10 deliverables completed during and submitted at the end of 10 of the 12 class periods. Students are required to select a topic by the end of the first class. From the second class meeting onwards, students sit with their groups. Students are provided 40 to 50 minutes of each class period to work on the various project deliverables. Since class time is leveraged for working on projects, the complexity, frequency, and scope of the deliverables can be extended and diversified, providing students with exposure to additional aspects of the ISDP.

This structure also enables the instructor to provide students feedback more frequently and in different modalities, which encourages critical thinking and allows students to improve the quality of their projects. While students work in their groups, the instructor circulates throughout the classroom answering questions, offering constructive assistance, and providing guidance.

An additional benefit of providing students with the opportunity to work on projects during class is that issues of unequal contributions, absenteeism, and free-riding are minimized. This approach ensures that the group collaborations remain on-track and equitable, providing a higher level of student participation and, ultimately, a higher quality of project submissions.

3. IMPLEMENTATION OF THE PROCESS-FOCUSED GROUP PROJECT

The features of the process-focused approach—such as the increased number of deliverables, reallocated class time, and shortened feedback loop—increase the complexity of administering this project. In order to deal with this complexity while also supporting student engagement, the structure of the project itself was modified in a number of ways. In this section, we describe how the process-focused group project is implemented, assessed, and supported.

Group Topic and Group Member Selection

The mode used to assign project topics and group members is an important component of the process-focused approach for group projects. Rather than having students propose topics, the instructor provides a list of topics related to various areas of student interest often associated with campus activities that students are able to select (see Appendix A for a list of topics). Since the topics list was developed by the instructor, this approach ensures that the topics used for group projects have sufficient breadth and complexity to reflect realistic ISDP. To encourage student engagement and interest, on the first day of class, the instructor introduces the topics, provides a brief synopsis of the project, and answers questions. Students then self-select into groups of five based on their interest in one of the topics. As students possess pre-existing interest in or experience with the topic, they can leverage domain knowledge, ultimately encouraging higher levels of student engagement over the entire course, and in turn, greater levels of student success. This approach enables the instructor to reinforce course concepts within the context of a topic that students are familiar with and can relate to.

Final Project Report and Reflection

In addition to the project deliverables due at the end of each class, on the last day of the course, each group submits a final project report and delivers a final presentation. This final report reinforces a core concept of SAD: the iterative development of a project. For the final project report, students combine the ten deliverables produced over the course of the semester into a cohesive system proposal. The instructions students receive for the final project are provided in Appendix B. To ensure student do not rush or poorly execute the creation of this final project report, they are encouraged to work on the report in parallel with each of the deliverables. The instructions for each deliverable include suggestions for how students can reconcile previous deliverables with what they have more recently developed. This approach ensures consistency and lack of contradiction across the different deliverables, and in turn, the components of the final report (for example, features in the system prototype that were not consistent with system requirements or the data model).

In addition to the project deliverables and final report and presentation, the groups submit a "reflection" section, where they reflect on what they learned through the process of working on this project. Having students complete this reflection further reinforces the process-focused approach to the project.

3.3. Learning Management System Support and Organization

The Learning Management System (LMS) is an important tool in supporting the additional complexity that the redesigned project entails. The LMS is used to create a structured learning environment that supports each phase of students' completion of the group project deliverables. To ensure that students collaborate during class with their group members to complete deliverables, assignments are only available the day and time of their associated class meeting. The group assignment function of the LMS is used to assign the deliverables, collect timely submissions, and ensure that instructor feedback is provided to the entire group.

The LMS provides students with an online space devoted to collaborations to share files and participate in project-related discussions. The advantage of using the LMS for group work is that the instructor can access a permanent record of all work, which can be useful for conflict resolution. To further support collaboration, students also use additional tools on their own, such as Google Docs for collaborative writing, along with Facebook to interact with group members outside of (and during) class.

4. CONCLUSIONS AND RECOMMENDATIONS

The process-focused approach to the group project has been successfully implemented six times in different class settings, including the flipped classroom approach and traditional lecture setup. We have observed a substantial increase in the quality of the projects students submitted compared to the outcome-focused approach. Our implementation of the process-focused group project in a SAD course has four key features that distinguish it from the outcome-focused approach. Each of these features have been incorporated with certain benefits in mind, though they also present particular challenges that need to be overcome.

The first feature is the increase in the number of deliverables from five to ten in the same course framework. This increase in deliverables enables students to examine the project in more detail, while providing them with the time necessary to understand the process of working on each deliverable. This approach enables students to work on an ISDP as a whole, rather than jumping from one disconnected deliverable to another. The challenge of this feature is that increasing the number of deliverables also increases the workload for both students and the instructor. This challenge can be overcome by efficient use of class time, leveraging the LMS (including use of rubrics), clear instructions, and an objective grading scheme. See Appendix C for the grading scheme.

The second feature of the process-focused approach are the modifications made to the wording and structure of each project deliverable. In essence, instead of merely describing the deliverables, the instructions provide prompts that guide students through the process of working in a group to make collective decisions regarding each deliverable and then communicating their vision using SAD tools. The student takeaway is how to work effectively in a group on an ISDP rather than generate a solution to a specific problem. The main challenge of this feature is that students can struggle with not having a definitively "correct" answer to the complex problem of an ISDP. To overcome this challenge, instructors can verbally reinforce that the point of the group project is not submitting the "correct solution," but rather working as a group to arrive at a "serviceable solution" and learning from the process rather than focusing on the end product.

The third feature of the process-focused approach to the group project is how class time is used. Working on group projects during class time requires a paradigm shift. Students have to adapt to a wholly different approach to group projects than what they may be used to. From the instructor's perspective, course content may have to be redistributed to accommodate reduced time for in-class instructions and other activities. Despite the adjustments required, however, the process-focused approach eliminates a significant number of issues associated with group projects. A common complaint among students assigned group projects outside of class is that conflict between group members can occur. However, when students work within the classroom's supervised environment, the instructor can address these conflicts through timely intervention. Students can also face challenges in scheduling meetings outside of class time due to varying class and work schedules, which can lead to students dividing up the assignment and working individually. Since students submit each deliverable at the end of a class period, they use class time to collaboratively discuss and develop project deliverables.

The fourth feature of the process-focused approach is the increased amount and types of feedback that the instructor is able to provide students. When students work on their projects during class, they are able to ask questions, clarify ideas, and receive timely verbal feedback as a group while developing their project. They also receive formal written feedback on their daily submissions before the next class meeting. This shortened and varied feedback loop supports and encourages student creativity and critical thinking, ultimately resulting in more nuanced and sophisticated project reports. One challenge of the open-ended nature of the ISDP is that students can be hesitant to present their ideas, and instead often mimic examples from the textbook or lectures. A benefit of the varied and in-person approach to feedback is that the instructor can take on a consultative role, guiding students in the direction of the project, alleviating their concerns, and encouraging creativity.

The process-focused approach can be used to supplement other outcome-focused projects, such as individual assignments that are completed outside of class that focus more on reinforcing the concepts, tools, and techniques that are being taught. As a result, students can benefit from both types of pedagogy. Through the implementation of these changes, we have observed that students have obtained a deeper understanding of the course concepts and have displayed higher levels of engagement in the class. Moreover, when compared to the outcome-focused approach, we have observed less variance in the quality of the project reports across the groups.

5. REFERENCES

Baepler, P. & Walker, J. D. (2014). Active Learning Classrooms and Educational Alliances: Changing Relationships to Improve Learning. *New Directions for Teaching & Learning*, 2014(137), 9-16.

Dennis, A., Wixom, B. H. & Tegarden, D. (2015). *Systems Analysis and Design: An Object-Oriented Approach with UML* (5th ed.). Hoboken, NJ: Wiley.

Favor, J. K. & Harvey, M. (2016). We Shall Not be Moved: Adult Learners' Intransigent Attitudes about Group Projects. *Adult Education Research Conference*.

Fuller, M. A., Valacich, J. S., George, J. F. & Schneider, C. (2010). *Information Systems Project Management: A Process and Team Approach* (1st ed.). Upper Saddle River, NJ: Prentice Hall.

Harris, R. (2007). A Systems Analysis and Design Semester Project: A Stand-alone Project vs a Competitive Project. *The Proceedings of the Information Systems Education Conference*, (24)3712, Pittsburgh, PA.

Lage, M. J., Platt, G. J., & Treglia, M. (2000). Inverting the Classroom: A Gateway to Creating an Inclusive Learning Environment. *Journal of Economic Education*, 31(1), 30-43.

Lumpkin, A. L., Achen, R. M., & Dodd, R. K. (2015). Student Perceptions of Active Learning. *College Student Journal*, 49(1), 121-133.

Melin, U., Axelsson, K., & Wedlund, T. (2006). Project Based Learning – An Emergent Framework for Designing Courses. *The Proceedings of the Information Systems Education Conference*, (23)2144, Dallas, TX.

Mukherjee, A. & Bleakney, S. (2015). Active Learning in a Collaborative Space: A Structured Approach to Increase Student Engagement in the Database Management Classroom. *The Proceedings of the Information Systems Education Conference*, 32, Orlando, FL.

Opdecam, E., Everaert, P., Keer, H., & Buysschaert, F. (2014). Preferences for Team Learning and Lecture-Based Learning among First-Year Undergraduate Accounting Students. *Research in Higher Education*, 55(4), 400-432.

Russell, J. & Russell, B. (2014). A Systems Analysis and Design Case Study for a Business Modeling Learning Experience for a Capstone CIS/IS Systems Development Class. *The Proceedings of the Information Systems Education Conference*, 31(3062), Baltimore, MD.

Stefanou, C., Stolk, J. D., Prince, M., Chen, J. C., & Lord, S. M. (2013). Self-Regulation and Autonomy in Problem- and Project-Based Learning Environments. *Active Learning in Higher Education*, 14(2), 109-122.

Thompson, K. J. & Beak, J. (2007). The Leadership Book: Enhancing the Theory-Based Connection through Project-Based Learning. *Journal of Management Education,* 31(2), 278-291.

Tsay, M. & Brady, M. (2010). A case study of cooperative learning and communication pedagogy: Does working in teams make a difference? *Journal of the Scholarship of Teaching and Learning*, 10(2), 78 – 89.

Waguespack, L. (1997). Threaded Live Case Study, Weaving Practice Through IS'97. *The Proceedings of the Information Systems Education Conference*, Orlando, FL.

Woods, D. M. & Howard, E. V. (2014). An IT Strategy Course: Why and How. *The Proceedings of the Information Systems Education Conference*, 31(3007), Baltimore, MD.

Woodward, B., Sendall, P., & Ceccucci, W. (2009). Integrating Soft Skill Competencies Through Project-based Learning across the Information Systems Curriculum. *The Proceedings of the Information Systems Education Conference*, 26(3762), Washington, D.C.

APPENDIX A: GROUP PROJECT TOPICS

GROUP PROJECT TOPICS

CHOOSE A PROJECT TOPIC

Please pick one of the nine topics described below for your group project. Please note the following regarding group membership.

- Students who choose the same topic will work together on the project for the entire module and may not change groups.
- Each group will contain a maximum of 5 students only, so membership is on a first-come first-serve basis.
- The instructor cannot add or remove students from the group.
- Students who do not choose a group by Jan 7 will not be assigned a group and will not receive any credit for the entire Group Project component of their course grade.

TOPIC LIST

- Find Me a Roommate
- Zoo Animal Management
- Gym Management Software
- Video Game Store
- Uber for Tutors
- Student Organization Management
- The Ultimate Travel Manager
- Fantasy Sport League Management
- Job Search Management

APPENDIX B: GROUP PROJECT REPORT AND PRESENTATION INSTRUCTIONS

GROUP PROJECT REPORT & PRESENTATION

REPORT

Your final report is a synthesis of all your previous deliverables. The most important aspect of this final report is that all the different sections should be consistent with each other. Your report should be presented in a professional manner and all the diagrams should be drawn using the notation shown in class and should be in black and white. Your diagrams can be landscape if they don't fit on the page in portrait mode. You can use the logo, colors and formatting from your initial branding exercise in your report. You must submit the report as a PDF.

GRADING CRITERIA

- **Presentation [20%]:** Points will be deducted for reports that are submitted in a non-professional format, if the diagrams are not black and white and if they use incorrect notation, if the cover sheet or table of contents are missing.
- **Completeness [40%]:** Points will be deducted if any sections are missing or incomplete.
- **Consistency [40%]:** Points will be deducted if your report lacks consistency.

PRESENTATION

As a group, you will also deliver a brief 8 minute presentation to the rest of the class summarizing your project report. You must convey your final report to the class with this presentation. The point of the presentation is to convey the most important and interesting aspects/features of your project using the different modeling tools that you have learned in this class.

GRADING CRITERIA

- **Presentation [20%]:** Points will be deducted if the presentation is not professional. Please practice presenting beforehand and make sure that you are audible at the back of the class.
- **Content [60%]:** Points will be deducted if the presentation does not cover all the important aspects of the project.
- **Reflection [10%]:** Points will be deducted if your group does not share the lessons you learned while working on the project.
- **Time Management [10%]:** Points will be deducted if your presentation goes over the prescribed 10 minute time limit or if the presentation is too short.

You may use Power Point slides for the presentation. If you choose to do this, please be sure to upload them to the class website before class begins on the day of presentations. All members of the group must be present on the day of the presentation and must participate during the group presentation.

DELIVERABLE

The following files should be uploaded to the assignments section on Canvas by 6pm.

One PDF Document [Download Sample]

One Power Point Presentation [Download Sample]

APPENDIX C: GRADING SCHEME

The group project is worth 30% of the final grade and distributed among the various deliverables as shown in the table below. The daily deliverables are low stakes (only 1% of the final grade) to motivate students to turn in the work in a timely fashion and stay on track with the group project. Additionally, the low stakes also serve to encourage the students to be more creative in their responses without the fear of adversely affecting their grades.

Class Meeting	**Project Deliverables**	**Grade**
1	Choose Group Topic	
2	GP#1:Group Introduction	1 %
3	GP#2:Project Plan	1 %
4	GP#3:System Abstract	1 %
5	GP#4:Requirements	1 %
6	GP#5:Process Model	1 %
7	GP#6:Class Diagram	1 %
8	GP#7:Use Cases	1 %
9	GP#8:Sequence Diagram	1 %
10	GP#9:Data Model	1 %
11	GP#10:Deployment Strategy	1 %
12	Final Report	10 %
	Final Presentation	10 %
	Total	30 %

Another advantage of the grading scheme is that students are assessed fairly for their contributions to group projects, which also ensures more equitable grading. For example, students only receive credit for the daily deliverables if they are present in class. Moreover, for the final project and presentation that makes up 20% of students' course grades, group members only receive credit if they attend and contribute to at least 50% of the daily deliverables, which prevents the common issue of free-riding in group projects.

APPENDIX D: SAMPLE GROUP PROJECT DELIVERABLE INSTRUCTIONS

To simulate stakeholder analysis, the project description includes role-playing activities where each student takes on the role of a different stakeholder and voices their expectations of the system. Following this role playing exercise, the group as whole consolidates these different expectations and writes a single requirements document that incorporates or at least addresses all the stakeholder opinions.

GROUP PROJECT #3: SYSTEM ABSTRACT

PART A: SYSTEM ABSTRACT [10 MIN - 1 PAGE]

Write a one page system abstract for your project. You should use the word document template that you created for Deliverable 1. Your system abstract must clearly describe the following:

- Purpose of the System: Describe the main purpose of this system.
- Basic Scope: Broadly outline the main features or sub-systems that comprise the system you are developing.
- Basic Design: What will your system architecture look like? This decision needs to take into consideration the types of users it will have, how they will use the system, on what types of devices, and how many users you will have. You may make use of symbols in this file if you wish to draw a diagram.

PART B: STAKEHOLDER ANALYSIS [25 MIN - 1 PAGE/STAKEHOLDER]

Identify at least 5 (one per group member) stakeholders for your project. Each group member should represent one of the stakeholders and must do the following:

- Give the stakeholder a name (e.g., Bob Roberts)
- List 5-10 things that the stakeholder might expect from the system.
- Moving forward with requirements gathering, how would you gather requirements from this stakeholder? Why?
- Explain your description to the rest of your group members. Do you find that there are conflicting expectations from the different stakeholders?

For the submission, write the description and details for each stakeholder. You should also indicate if there are any conflicting or contradictory requirements. Each stakeholder should be on a separate page.

DELIVERABLE

The following files should be uploaded to the assignments section on Canvas by 6pm.

One Word Document. [Sample Submission - This would get a grade of 7/10]

FOR NEXT CLASS

You must do the following before your group meeting during the next class period:

- Think about the functional and non-functional requirements for your system.
- Think about what the user interfaces for your system look like?

Dotting i's and Crossing T's: Integrating Breadth and Depth in an Undergraduate Cybersecurity Course

David J. Yates
dyates@bentley.edu

Mark Frydenberg
mfrydenberg@bentley.edu

Leslie J. Waguespack
lwaguespack@bentley.edu

Isabelle McDermott
mcdermo_isab@bentley.edu

Jake OConnell
oconnel_jake@bentley.edu

Frankie Chen
chen_fran@bentley.edu

Computer Information Systems Department
Bentley University
Waltham, MA

Jeffry S. Babb
jbabb@wtamu.edu
Computer Information and Decision Management Department
West Texas A&M University
Canyon, TX

Abstract

The importance of updating, expanding and improving what is taught in cybersecurity curricula is increasing as the security threat landscape becomes more dangerous, breaches become more frequent, and the number of deployed Internet of Things (IoT) devices, known for their security challenges, grows exponentially. This paper argues that a profile of "T-shaped" skills, which is known to be desirable in many consulting and design professions, is being reflected in the latest manifestations of cybersecurity curriculum design and accreditation. A model of learning that yields "T-shaped" professionals combines the ability to apply knowledge across domains (breadth) with the ability to apply functional and disciplinary skills (depth). We present the design of a junior- or senior-level cybersecurity course in which the horizontal stroke of the "T" (representing breadth) spans knowledge areas that cut across the people, process and technology triad. The vertical stroke of the "T" (representing depth) is provided by two aspects of the course design: first, learning the foundational principles of cybersecurity, including practical examples from cryptography and network security; and second, applying the principles of cybersecurity to a semester project, allowing students to expand the core "T" of the course to satisfy their own passions and interests. Our paper concludes with student and instructor reflections on the implementation of this cybersecurity course, as well as broader implications of the lessons learned after the initial offering of this course.

Keywords: Cybersecurity curricula, cybersecurity education, knowledge areas, security accreditation, cybersecurity course design, T-shaped knowledge and skills, security certification.

1. INTRODUCTION

Cybersecurity as a field of study began as soon as computers transitioned from stand-alone devices to being connected directly to a network, or to another device that is connected to a network. Thus, what we know today as cybersecurity began at the intersection of computer security (Bishop, 2018) and network security (Stallings, 2017). As computing and networks have become pervasive, security concerns have expanded to include application security, database security, infrastructure security, cloud, web and mobile security, and similar topics. Today information security and cybersecurity are two distinct, but related, umbrella disciplines that reflect the union of many areas of security.

Information security is defined in Andress (2014) as "'protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction' according to U.S. law." [p. 3]

Cybersecurity (sometimes written as *Cyber security*) is defined in Burley & Bishop et al. (2017) as a "computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management." [p. 16]

These definitions suggest that security (in the large) is inclusive of many areas that are broad in their own right, e.g., computing, engineering, communication, human factors, law, ethics, policy, psychology, sociology, management, and even economics (Anderson, 2001). Hence attempts to disentangle one area within cybersecurity from another is like trying to separate and transplant one part of a Banyan Tree from another (see Figure 1).

The analysis, insights and reflections in this paper are, in part, a call to action to college and universities to develop and deliver the knowledge and skills that are needed to prepare their graduates for one of the many possible careers that fall under the cybersecurity umbrella (Newhouse, Keith, Scribner, & Witte, 2017; NIST, 2018; NSA, 2018a; Singer & Friedman, 2014).

Figure 1. Banyan Tree photographed on Oahu, Hawaii

This study focuses on the design and implementation of an undergraduate cyber-security course based on the Burley and Bishop et al. (2017) definition presented above. In describing and illustrating this design, and also considering implications for accreditation and certification, we observe that a profile of knowledge and skills that yields "T-shaped people" (Guest, 1991; Brown, 2009; Sandeen & Hutchinson, 2010) is being reflected in the latest recommendations for cybersecurity education in academia as well in practice.

2. T-SHAPED KNOWLEDGE AND SKILLS

In our application of a T-shaped model of knowledge and skills (Madhavan & Grover, 1998; Peters, 2012) to cybersecurity, the horizontal bar of the "T" represents breadth and spans knowledge areas that cut across the people, process and technology triad (Andress, 2004). The vertical bar of the "T" represents depth and is based on the foundational principles of cybersecurity based in computing disciplines (Parekh & DeLatte, 2018). Furthermore, these foundational principles are strengthened by pairing them with practical examples from cryptography (Stallings, 2017), computer security (Bishop, 2018) and network security (Kaufman, Perlman, & Speciner, 2002).

The next section of the paper describes the T-based model for our cybersecurity course design and relates the course content to the latest curricula guidelines (Burley & Bishop, 2017). These guidelines reflect a two-year collaboration among the ACM, IEEE (CS), AIS (SIGSEC) and

IFIP. We then describe how students taking the course augmented the knowledge and skills embedded in the core "T" of the course with depth in specific areas developed as part of a course project. We conclude with an analysis of the current state of cybersecurity accreditation, reflections on the student and instructor experiences of the course, and finally offer our thoughts on improving or adapting the course at the center of this study in different ways.

3. COURSE DESIGN AND IMPLEMENTATION

Both cybersecurity and information security are multidisciplinary fields of study. Table 1 (see below) and Appendix A make this case for cybersecurity, which includes concepts as diverse as security design principles, digital forensics, identity management, and cyber ethics, among many others. Likewise, Crowley (2003) summarizes more than 24 important content areas included in U.S. government and commercial efforts to provide educational guidance to professionals working in, or students aspiring to work in, information security. Not surprisingly, factoring just one course from the eight cybersecurity Knowledge Areas (KAs) shown in Table 1 was challenging. The solution to this challenge required an integrated design (Iansiti, 1995) connecting the breadth of the course (the holistic, multidisciplinary horizontal bar in Figure 2) to the depth of the course (the technical vertical bar in Figure 2) and vice-versa.

Note that the KAs in Table 1 are listed in order from the lowest level (i.e., data and software security) to the highest level (i.e., organizational and societal security).

Data Security	Software Security	Component Security
Connection Security	System Security	Human Security
Organizational Security	Societal Security	

Table 1. Knowledge Areas (KAs) in 2017 ACM, IEEE (CS), etc. JTF Undergraduate Curriculum Guidelines, aka (Burley & Bishop, 2017)

The horizontal stroke of the "T" in Figure 2 includes people, process and technology concerns (Andress, 2004). The vertical stroke is dominated by technology concerns. Brown (2009) would describe a person with fluency in relating and connecting areas on the horizontal in Figure 2 as an integrative thinker and skilled generalist and a person with fluency in all areas on the vertical as a deep thinker and skilled specialist (a so-called "i"). An ideal person (e.g., employee, consultant or designer) in most socio-technical realms has T-shaped knowledge and skills that enable her to think adaptively and to move seamlessly between being a skilled generalist and a skilled specialist (Brown, 2009).

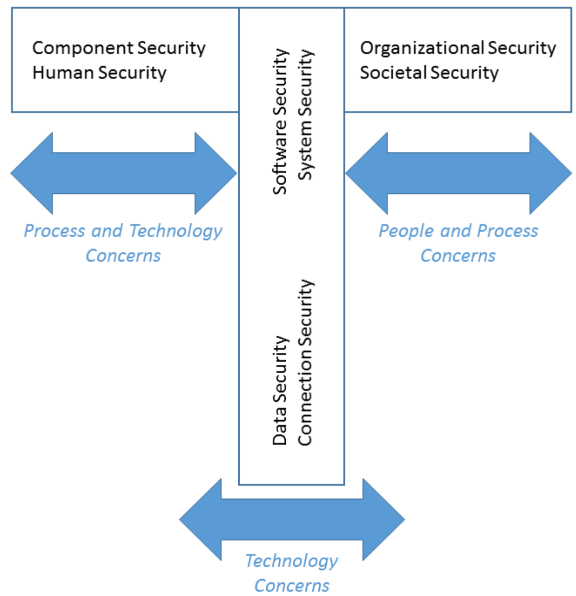


Figure 2. Cybersecurity Knowledge Areas organized in a "T" reflecting holistic, multi-disciplinary breadth and technical depth

The cybersecurity course offered at Bentley University was intended to teach students cybersecurity principles and practices, favoring technical content over non-technical content. Using the disciplinary lenses summarized in Burley and Bishop et al. (2017), the syllabus presented in Appendix B reflects the mostly technical computing disciplines in the approximate percentages shown in Figure 3. Although Figure 2 is our own creation, the graphic component of Figure 3 – showing inter-disciplinary content from at least five domains plus five computing disciplines – is recreated from Figure 2 in Burley & Bishop et al. (2017).

In an "i-shaped" course design, students develop deep skills and experience in one area but may not apply or connect those skills to other areas or disciplines. Although the percentages in Figure 3 might suggest an "i-shaped" cybersecurity course design, the textbook for the course selectively presented people and process as well as technical concerns. The technical areas we covered in eleven chapters in Stallings (2017) were mostly grounded in discrete mathematics, computer science and computer engineering.

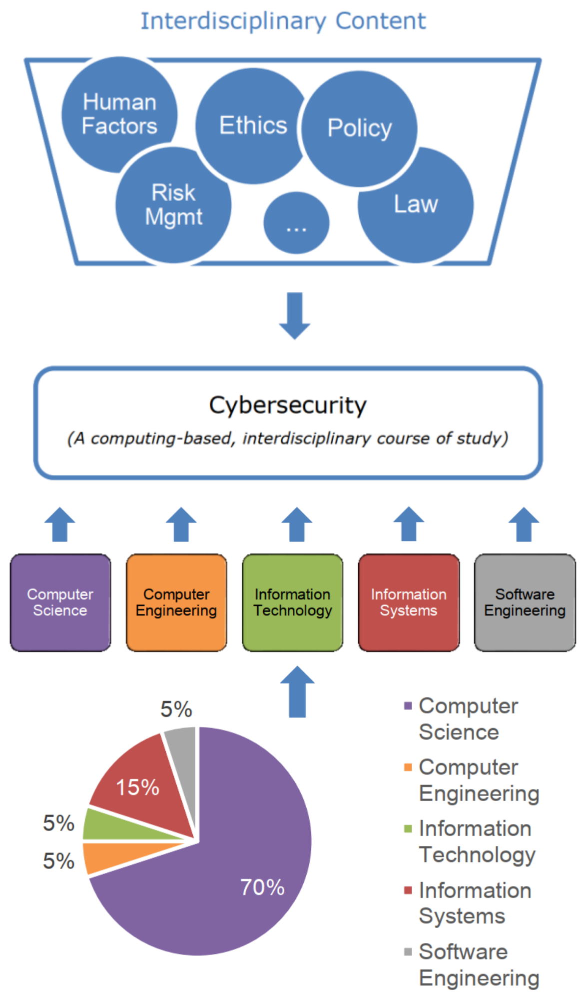


Figure 3. Disciplinary lens for Bentley University CS 401 cybersecurity course

The CS 401 course offered at Bentley University transitioned from textbook readings to supplemental readings in Week 12. Two of the five supplemental readings were grounded in information systems and information technology (NIST, 2018; US DHS, 2016). The other three supplemental readings (Bonneau & Miller, 2015; Chen, Paxson, & Katz, 2010; Nakamoto, 2008) were grounded in computer science and software engineering. Taken together these six resources yielded the T-shaped course implementation shown in Figure 4. Note that Figure 4 duplicates the Knowledge Areas cast as a "T" in Figure 2, but adds the week-by-week coverage (listed as red numbers ranging from 1 to 14) shown in the course syllabus from the Spring 2018 rendition of CS 401.

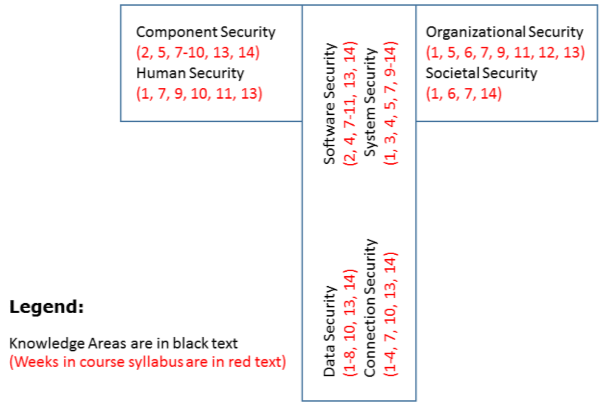


Figure 4: Bentley University CS 401 cybersecurity course "T" implementation annotated with week-by-week coverage detailed in Appendix B

The CS 401 course was offered as a directed study for three conscientious students, all of whom are Computer Information Systems majors, during their junior or senior year at Bentley University. U.S. News and World Report ranked Bentley University highly as an internationally recognized business university with "more selective" admission standards in 2018. The syllabus presented in Appendix B, including the selection of textbook and readings, is therefore designed for above average (or stronger) undergraduate students. This means that although the cybersecurity course design reflected in Table 1 and Figure 2 is easily portable to other technical-focused curricula, the implementation reflected in Figure 3 and Figure 4 may or may not be.

We now turn our attention to the three cybersecurity course projects that counted for 45% of each student's grade in CS 401. Although these projects were developed and submitted in phases as individual projects, similar team course projects -- adapted to local pedagogical norms -- could be developed for larger class sizes.

4. BENTLEY UNIVERSITY CS 401 STUDENT PROJECTS

An important goal of student projects in CS 401 was applying the principles of cybersecurity in a semester project. The projects also served two additional goals. First, the project allowed students to expand the core "T" of the course to satisfy their own passions and interests. For McDermott and OConnell, this meant understanding how machine learning can be applied to improve cybersecurity. For Chen, this meant exploring how the security features of blockchain technology can be leveraged to transform business processes. Second, having students conduct independent research reinforces some of the essential cybersecurity concepts listed in Appendix A within a specific area. Thus, while the core "T" for every student in CS 401 was as summarized in Figure 4, the semester projects added depth in a way that customized the learning outcomes for each student as shown in Figure 5.

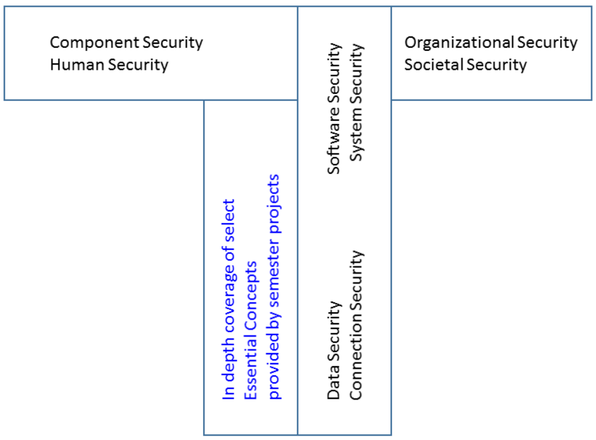


Figure 5. CS 401 cybersecurity course "T" modified by select Essential Concepts from Appendix A

The title and a brief summary of each student project are presented below, followed by the six most prominent Essential Concepts (ECs, Burley & Bishop, 2017) covered by each project.

The ECs reinforced by the student projects were quite different. Two ECs are common to the McDermott and Chen projects – data integrity and authentication, and personal data privacy and security – and one EC – system monitoring – was common to the McDermott and OConnell projects.

***McDermott*. Malware Identification and Protection on Mobile Devices Using Machine Learning**

This study reviews the current landscape of anti-malware security on Android mobile devices in the United States. There have been major breaches in confidentiality in recent years on smartphones, and there is now an increased need for safety due to users' reliance on these devices. Based on current security standards, the requirements and expectations of users were discussed with regard to how they affect what security must be on a system. Google's existing machine learning protocols in security were also reviewed. This study proposes the use of new machine learning methodologies to solve the four main issues (1) identification of mobile device vulnerabilities, (2) patching of vulnerabilities, (3) identification of malware on a device, (4) ways to remove malware from devices. The concepts of red-teaming, alerts, reinforcement machine learning, and virtual memory access patterns were covered as suggested ways to solve these issues. The implementation of these is described and an analysis of the "Googligan" malware problem is reviewed with respect to these concepts.

Most Significant ECs for McDermott: Data integrity and authentication; Security requirements and their role in design; Static and dynamic testing; Configuring and patching; Personal data privacy and security; System monitoring

***OConnell*. The Effectiveness of Behavior-Based Access Control: Mitigating Internal Threats at U.S. Financial Institutions**

Internal cyber threats at U.S. financial institutions present a significant concern due to the advantage held by insiders and the value of financial data and infrastructure. Currently, authorization management handled through traditional access control methods is insufficient for the dynamic networks and organizational systems of the twenty-first century. In response, behavior-based access control has been proposed as a solution, offering a dynamic and automatic access control system. To broaden our understanding of internal threats and the related benefits of behavior-based access control, this research aimed to 1) summarize the importance of considering internal threats, 2) identify the state of the art in behavior-based access control and its role in internal threat mitigation, 3) define challenges associated with the state of the art, and 4) present strategic practices and considerations for implementing these systems with consideration for financial organizations. This research aims to inform the evaluation of behavior-based access control and to provide background and considerations for decision makers determining whether to implement a system of this type.

Most Significant ECs for OConnell: Access control; Social behavioral privacy and security; Social engineering; Software component interfaces; System monitoring; Risk management

***Chen*. Adoption of Blockchain Technology: The Healthcare Industry vs. Retail Industry**

Because of its potential to disrupt financial services and other industries, blockchain technology has the ability to be the 'next internet'. The inherent benefits of built-in security coupled with the flexibility in different implementations allows for many applications and use cases. The acceptance of blockchain technology depends largely on the industry, its regulations, the use cases, and their relevant benefits. Blockchain technology was analyzed with respect to its benefits, risks, strengths and weaknesses in the context of two specific industries. The two industries explored are the healthcare industry, with a focus on healthcare data for the FDA and CDC, and the retail industry, with a focus on supply chain management for Walmart and Amazon. These two industries are used to assess the potential benefits and risks of blockchain by examining the opportunities and challenges in applicable use cases. This study concludes by formulating an outlook for blockchain adoption by these industries.

Most Significant ECs for Chen: Basic cryptography concepts; Data integrity and authentication; Personal data privacy and security; Governance and policy; Laws, ethics, and compliance; Supply chain management security

As can now be seen, the students participating in this course had varying focuses in their topics. Using the “T” shaped knowledge and skills provided by the course design, the students were able to develop and integrate these in very different ways. In a larger course setting this may lead to students having very similar knowledge areas enumerated within their “T”s, but there would likely be varying depths at which these topics are learned. In this example course, the students that had overlapping KAs almost certainly would give differing explanations of how these were integrated into their course projects.

We now explore issues beyond courses and projects. From an institutional perspective, we analyze and assess the current state of cybersecurity accreditation in the next section. From an educational perspective, we consider post-secondary certifications that are potentially helpful to students that pursue a career in cybersecurity in Appendix D.

5. ACCREDITATION

Cybersecurity accreditation is a work-in-progress (ABET, 2017; Yang & Wen, 2017; Wescott & Clark, 2017). ABET’s efforts to date have focused on six of the eight Knowledge Areas shown in Table 1, i.e. all except Component Security and Connection Security (ABET, 2017; Burley & Bishop, 2017; Wescott & Clark, 2017). It is an open question if these last two KAs will be added to the scope of ABET’s cybersecurity accreditation. AACSB’s efforts to date have been based on IS 2010. Within IS 2010, six of the seven core courses list some aspect of security as an important topic area:

- Foundations of Information Systems;
- Data and Information Management;
- Enterprise Architecture;
- IT Infrastructure;
- Systems Analysis and Design; and
- IS Strategy, Management, and Acquisition.

Furthermore, IS 2010 lists “IT Security and Risk Management” as one of a handful of important IS electives.

As of this writing, the most useful accreditation tools we have in the United States are the Center of Academic Excellence (CAE) designations from the National Security Agency (NSA, 2018b). The most popular of these designations is for Cyber Defense (CD).

The horizontal bar in Figure 6 contains what the NSA and Department of Homeland Security (DHS) call foundational KUs whereas the vertical bar contains *core non-technical KUs* (NSA, 2018a). Yang and Wen (2017) focus on non-technical NSA CAE-CD knowledge and skills in their study, as depicted in Figure 6, because of the connection between these eight Knowledge Units (KUs) and AACSB accreditation.

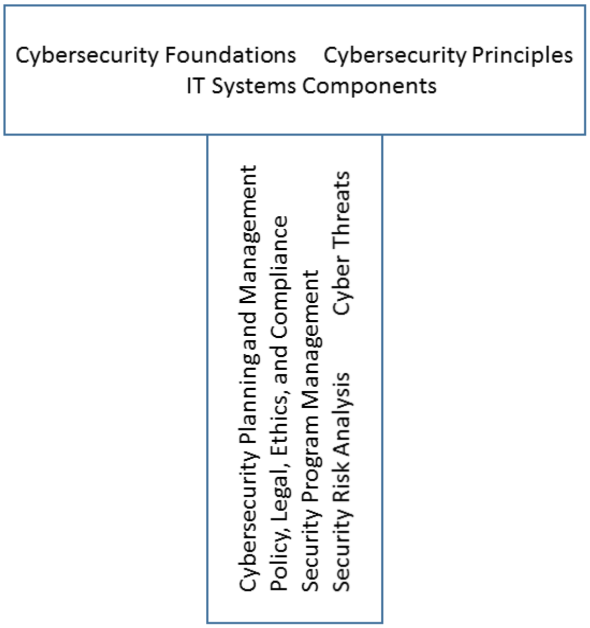


Figure 6. National Security Agency (NSA) Cyber Defense (CD) foundational and non-technical core Knowledge Units (KUs)

Institutions more focused on technical than managerial or behavioral knowledge and skills can leverage the NSA CAE-CD KUs shown in Figure 7. The horizontal bar in Figure 7 also contains the NSA's three foundational KUs whereas the vertical bar contains five *core technical KUs* (NSA, 2018a). One of the strengths of NSA CAE-CD KUs is how comprehensive they are (Yang & Wen, 2017). In addition to the three foundational and ten core KUs shown in Figure 6 and Figure 7, institutions are encouraged to extend their offerings to include other KUs organized around specific focus areas (NSA, 2018a). Appendix C lists the 57 "optional" KUs that the NSA provides as guidance.

Finally, Westcott and Clark (2017) highlight the importance of ensuring that cross-cutting concepts are thoughtfully integrated into cybersecurity curricula for both pedagogical and accreditation purposes. For decades, these have included confidentiality, integrity and availability; the so-called CIA triad. Burley and Bishop et al. (2017) suggest that there is a need to expand this list of concepts from three to at least six:

- Confidentiality;
- Integrity;
- Availability;
- Risk;
- Systems thinking; and
- Adversarial thinking.

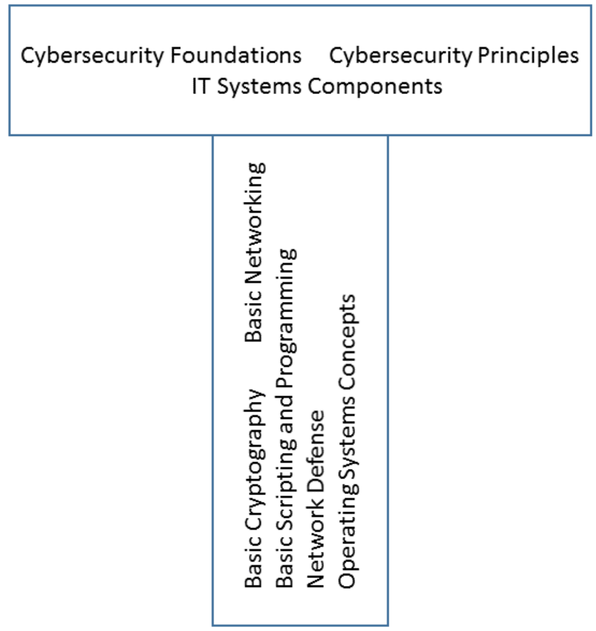


Figure 7. National Security Agency (NSA) Cyber Defense (CD) foundational and technical core KUs

6. IMPLICATIONS AND CONCLUDING REMARKS

With some exceptions, if a science and technology story appears on the cover of Time Magazine (Vella, 2018) and is within a computing discipline, we should reflect on if and how we teach the topic at hand. This 2018 Time Special Edition does a nice job of presenting cybersecurity in a way that is accessible to its target audience and features actionable checklists for things that one should do at home (and at work) to improve one's cybersecurity. But what do administrators and faculty need to understand about cybersecurity? We offer our reflections here with the understanding that these represent a more academic perspective than those of Time Magazine.

Implications for Administrators

Cybersecurity is emerging as a distinct discipline, even though it is tightly connected to all five of the computing disciplines shown in the lower half of Figure 3 as well as others, e.g., security analytics (Talabis, McPherson, Miyamoto, & Martin, 2015). This suggests that colleges and universities need to consider updating and revising curricula and courses in ways that go far beyond the security knowledge areas that their faculty learned as students (Newhouse, Keith, Scribner, & Witte, 2017; NIST, 2018). Although beyond the scope of our study, it is also important to consider the multidisciplinary nature of cybersecurity as suggested by the interdisciplinary content examples shown at the top of Figure 3. We expect that many institutions can offer compelling, interesting and valuable courses that integrate two or more disciplines, e.g., human factors and cybersecurity; or policy, law, ethics and security; etc.

Because cybersecurity is an emerging discipline, the state of accreditation for cybersecurity is in flux. We recommend that administrators track the state of cybersecurity accreditation hand-in-hand with tracking advances and changes to curricula as they develop. For now, this likely means tracking ABET's and AACSB's activity and their progress in this area. There are also good reasons to consider applying for a National Security Agency Center of Academic Excellence in Cyber Defense or Cyber Operations (NSA, 2018b). Obtaining and supporting these designations (i.e., NSA CAE-CD and NSA CAE-CO), however, clearly will require institutional resources.

Implications for Faculty

Faculty teaching in computing disciplines are on the front lines of addressing what Simson Garfinkel calls "The Cybersecurity Mess," which accurately describes the current state of affairs (Garfinkel, 2016; Vella, 2018). We encourage faculty to carefully consider the knowledge and skills they might design into their own "T-shaped" cybersecurity course, tailored to the institution or organization offering the course. Important questions here are how a course design matches the needs of the students as well as the requirements of their prospective employers. For the same stakeholders, it is also important to strike the right balance of technical and non-technical course content. Like the parts of a Banyan Tree (see Figure 1), the technical and non-technical components of cybersecurity are woven together and interconnected, as they are in information security (Cram & D'Arcy, 2016).

Faculty that are outside computer science departments can still add tremendous value by teaching their students cybersecurity using a T-shaped model. Applying this approach to course design and pedagogy will allow students to be more aware of the connections between domains, and also how they fit into knowledge areas. Integrating non-technical and interdisciplinary skills in courses outside of CS provides the opportunity to create more well-rounded students that understand how different essential concepts and topics can come together.

Concluding Remarks

More than 3 billion people are online (including bad actors) and more than 30 billion Internet of Things devices soon will be directly or indirectly connected to the internet. Furthermore, the digital transformation of modern enterprises makes information and communication technology (ICT) infrastructure mission critical. This ICT infrastructure therefore needs securing using a robust, holistic, and multidisciplinary approach, hence the horizontal stroke in our "T". But what about the vertical stroke in our "T"? From a science and technology perspective, cryptography and network security, as conceived in CS 401, are central to this urgent need.

In hindsight, we were pleased with the main text used in CS 401 (Stallings, 2017). As the title suggests, the strongest aspects of the Stallings (2017) book are its treatment of cryptography and network security. It is also adequate for teaching the basics within six of the eight cybersecurity Knowledge Areas shown in Table 1. It falls short, however, in providing adequate material for teaching organizational security and societal security. Another book that is just as technical as Stallings (2017) but provides broader coverage is Bishop (2018). Different books might be better for less technical Computer Information Systems majors than McDermott, OConnell and Chen. For example, the texts (Pfleeger & Pfleeger, 2011) and (Whitman, Mattord, & Green, 2013) are explicitly mentioned as good examples in CS 2013 (Sahami & Roach, 2013). A different book would almost certainly be better for a more applied IS or IT major (Misra & Khurana, 2017). Three such examples are (Andress, 2014), (Boyle & Panko, 2014) and (Vacca, 2017). For minors in a computing discipline, Meeuwisse (2017) is an up-to-date and interesting alternative.

The supplemental readings for CS 401 in part balanced out the "T" shown in Figure 4. Only two of the five readings, however, were foundational in that they covered security operations at a high-level (NIST, 2018) and secure, tamper-resistant transactions, by example (Nakamoto, 2008). The remaining supplemental readings covered timely or more advanced topics (Bonneau & Miller, 2015; Chen, Paxson, & Katz, 2010; US DHS, 2016). If we were to teach this cybersecurity course again, supplemental readings that covered organizational security and societal security in general, and privacy in particular (Solove, 2010), would be welcome additions.

The authors are instructors or students at business schools in which management and governance of organizations is covered elsewhere in our respective curricula. However, special treatment of cybersecurity is inadequate or outdated in the courses at Bentley University and

West Texas A&M University, as we imagine it is in similar courses at other business schools that cover management, governance, or risk. Thus, teaching cybersecurity appears to be a critical area in which we can better serve our students. This paper is our attempt at raising awareness of the importance of teaching cybersecurity within a computing discipline and presents our approach to doing so mindfully. It remains an open question where cybersecurity fits in the landscape of higher education beyond computing disciplines. Furthermore, as younger generations are growing up as digital natives, we should also be asking what aspects of cybersecurity need to be taught in high school, middle school, or elementary school.

7. REFERENCES

Accreditation Board for Engineering and Technology (ABET). (2017). *ABET Seeks Feedback on Proposed Accreditation Criteria for Cybersecurity Academic Programs.* Baltimore, MD. Retrieved from http://abet.org/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-academic-programs/

Anderson, R. (2001). Why information security is hard - An economic perspective. *17th Annual Computer Security Applications Conference*, (pp. 358-365). New Orleans, LA.

Andress, A. (2004). *Surviving Security: How to Integrate People, Process, and Technology* (2nd ed.). Boca Raton, FL: CRC Press.

Andress, J. (2014). *The Basics of Information Security* (2nd ed.). Rockland, MA: Syngress.

Bishop, M. (2018). *Computer Security: Art and Science* (2nd ed.). Boston, MA: Addison-Wesley Professional.

Bonneau, J., & Miller, A. et al. (2015). *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.* International Association for Cryptologic Research. Retrieved from https://pdfs.semanticscholar.org/88a6/03ffe828c503b6818410bdb3dae435f90ebe.pdf

Boyle, R. J., & Panko, R. R. (2014). *Corporate Computer Security* (4th ed.). Boston, MA: Pearson.

Brown, T. (2009). *Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation.* New York, NY: Harper Business.

Burley, D. L., & Bishop, M. et al. (2017). *Cybersecurity Curricula 2017.* New York, NY: ACM.

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC)^2 CISSP Certified Information Systems Security Professional Official Study Guide* (8th ed.). Indianapolis, IN: Sybex.

Chen, Y., Paxson, V., & Katz, R. H. (2010). *What's New About Cloud Computing Security?* Tech. Report UCB/EECS-2010-5, Dept. of Electrical Engineering and Computer Sciences. Berkeley, CA: University of California.

Cram, W. A., & D'Arcy, J. (2016). Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future. *Communications of the Association for Information Systems, 39*, Article 3.

Crowley, E. (2003). Information System Security Curricula Development. *ACM Conference on Information Technology Curriculum*, (pp. 249-255). Lafayette, IN.

Dennis, A. R., & Minas, R. K. (2018). Security on Autopilot: Why Current Security Theories Hijack our Thinking and Lead Us Astray. *ACM SIGMIS Database, 49*(SI), 15-38.

Garfinkel, S. (2016). The Cybersecurity Mess, Retrieved from https://simson.net/page/Main_Page. Washington, DC.

Georg, G., & Ray, I. et al. (2009). An Aspect-Oriented Methodology for Designing Secure Applications. *Information and Software Technology, 51*(5), 846-864.

Grover, M., Reinicke, B., & Cummings, J. (2015). How secure is education in Information Technology? A method for evaluating security education in IT. *Proceedings of the EDSIG Conference.* Wilmington, NC.

Guest, D. (1991, September 17). The hunt is on for the Renaissance Man of computing. *The Independent*.

Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical Hacking: Educating Future Cybersecurity Professionals. *Proceedings of the EDSIG Conference.* Austin, TX.

Iansiti, M. (1995). Technology integration: Managing technological evolution in a complex environment. *Research Policy, 24*, 521-542.

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security: Private Communication in a Public World* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Madhavan, R., & Grover, R. (1998). From Embedded Knowledge to Embodied Knowledge: New Product Development as

Knowledge Management. *Journal of Marketing, 62*(4), 1-12.

Meeuwisse, R. (2017). *Cybersecurity for Beginners* (2nd ed.). Hythe, UK: Cyber Simplicity.

Misra, R. K., & Khurana, K. (2017). Employability Skills among Information Technology Professionals: A Literature Review. *Procedia Computer Science, 122*, 63-70.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Retrieved from https://bitcoin.org/bitcoin.pdf.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* Washington, DC.

National Security Agency (NSA). (2018a). *Centers of Academic Excellence in Cyber Defense (CAE-CD) 2019 Knowledge Units.* Ft. George G. Meade, MD.

National Security Agency (NSA). (2018b). *What is a Center of Academic Excellence (CAE)?* Ft. George G. Meade, MD. Retrieved July 15, 2018, from https://nsa.gov/resources/ students-educators/centers-academic-excellence/

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, Special Publication 800-181.* Washington, DC: U.S. National Institute of Standards and Technology (NIST).

O'Hara, B. T., & Malisow, B. (2017). *CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide.* Indianapolis, IN: Sybex.

Parekh, G., & DeLatte, D. et al. (2018). Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education, 61*(1), 11-20.

Peters, J. (2012). Educating Designers to a T. *Design Management Institute Review, 23*(4), 62-70.

Pfleeger, C. P., & Pfleeger, S. L. (2011). *Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach.* Upper Saddle River, NJ: Prentice Hall.

Ross, R., McEvilley, M., & Oren, J. C. (2018). *Systems Security Engineering, Special Publication 800-160, Volume 1.* Washington, DC: U.S. National Institute of Standards and Technology (NIST).

Sahami, M., & Roach, S. et al. (2013). *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science.* New York, NY: ACM.

Sandeen, C. A., & Hutchinson, S. (2010). Putting Creativity and Innovation to Work: Continuing Higher Education's Role in Shifting the Educational Paradigm. *Continuing Higher Education Review, 74*, 81-92.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York, NY: Oxford University Press.

Solove, D. J. (2010). *Understanding Privacy.* Cambridge, MA: Harvard University Press.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Boston, MA: Pearson.

Talabis, M., McPherson, R., Miyamoto, I., & Martin, J. (2015). *Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data.* Waltham, MA: Syngress.

Topi, H., & Valacich, J. S. et al. (2010). *Curriculum Guidelines for Undergraduate Degree Programs in Information Systems (IS 2010).* Atlanta, GA: Association for Information Systems.

U.S. Department of Homeland Security. (2016). *Strategic Principles for Securing the Internet of Things, Version 1.0.* Washington, DC.

Vacca, J. R. (2017). *Computer and Information Security Handbook* (3rd ed.). Burlington, MA: Morgan Kaufmann.

Vella, M. (2018). *Cybersecurity: Hacking, the Dark Web and You.* New York, NY: Time Books.

Wescott, J., & Clark, U. (2017). Cyber Defense Education & A Linux Toolkit. *Proceedings of the EDSIG Conference.* Austin, TX.

Whitman, M. E., Mattord, H. J., & Green, A. (2013). *Hands-On Information Security Lab Manual* (4th ed.). Boston, MA: Cengage.

Yang, S. C., & Wen, B. (2017). Toward a Cybersecurity Curriculum Model for Undergraduate Business Schools: A Survey of AACSB-accredited Institutions in the United States. *Journal of Education for Business, 92*(1), 1-8.

Appendix A – Joint Task Force on Cybersecurity Education Knowledge Areas [From CSEC 2017 Report aka (Burley & Bishop, 2017)]

Knowledge Area	Knowledge Units	Essential Concepts
Data Security	Cryptography Digital Forensics Data Integrity and Authentication Access Control Secure Communication Protocols Cryptanalysis Data Privacy Information Storage Security	Basic cryptography concepts Digital forensics End-to-end secure communications Data integrity and authentication Information storage security
Software Security	Fundamental Principles Design Implementation Analysis and Testing Deployment and Maintenance Documentation Ethics	Fundamental design principles including least privilege, open design, and abstraction Security requirements and their role in design Implementation issues Static and dynamic testing Configuring and patching Ethics, especially in development, testing and vulnerability disclosure
Component Security	Component Design Component Procurement Component Testing Component Reverse Engineering	Vulnerabilities of system components Component lifecycle Secure component design principles Supply chain management security Security testing Reverse engineering
Connection Security	Physical Media Physical Interfaces and Connectors Hardware Architecture Distributed Systems Architecture Network Architecture Network Implementations Network Services Network Defense	Systems, architecture, models, and standards Physical component interfaces Software component interfaces Connection attacks Transmission attacks
System Security	System Thinking	Holistic approach

	System Management System Access System Control System Retirement System Testing Common System Architectures	Security policy Authentication Access control Monitoring Recovery Testing Documentation
Human Security	Identity Management Social Engineering Personal Compliance with Cybersecurity Rules / Policy / Ethical Norms Awareness and Understanding Social and Behavioral Privacy Personal Data Privacy and Security Usable Security and Privacy	Identity management Social engineering Awareness and understanding Social behavioral privacy and security Personal data privacy and security
Organizational Security	Risk Management Security Governance and Policy Analytical Tools Systems Administration Cybersecurity Planning Business Continuity, Disaster Recovery, and Incident Management Security Program Management Personnel Security Security Operations	Risk management Governance and policy Laws, ethics, and compliance Strategy and planning
Societal Security	Cybercrime Cyber Law Cyber Ethics Cyber Policy Privacy	Cybercrime Cyber law Cyber ethics Cyber policy Privacy

Appendix B – Cybersecurity Course Syllabus

Bentley University – Computer Information Systems Department

CS 401 – Cybersecurity

Spring 2018 Syllabus

Instructor: David J. Yates
E-Mail: dyates@bentley.edu
Class Meeting: Monday & Thursday 11:00 AM – 12:20 PM
Location: Our classroom
Office Hours: By appointment

Course Overview

Prerequisites

A networking, operating systems or computer architecture course.

Required Materials

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice,* 7th Edition. Hoboken, New Jersey: Pearson Education.

In addition to the required textbook, supplemental readings and other material will be provided on Blackboard.

Course Description

This course provides a technical focus on information, computer, and network security, which together form the basis for cybersecurity. It introduces what cybersecurity means, both in the abstract and in the context of real-world information systems. Students learn relevant cybersecurity principles, practices, technologies, and approaches. Students recognize and understand threats to confidentiality, integrity and availability as well as best-practices to defend against such threats.

Course Objectives

Upon successful completion of the course and the assignments, it is expected that the student will:

1. Develop a basic understanding of cybersecurity, how it has evolved, and best practices for cybersecurity used in modern enterprises.
2. Develop an understanding of cybersecurity as practiced in hardware, operating systems, virtual machines, distributed information systems, networks, and representative applications.
3. Gain familiarity with prevalent network and system attacks, defenses against them, and forensics to investigate the aftermath.

4. Develop an understanding of security policies as well as mechanisms to implement and assure such policies.

Teaching Methods

1. Lectures and Discussion: Important material from the class notes and outside sources will be covered in class. Students should plan to take careful notes as not all material can be found in the handout class notes or class examples. Discussion is strongly encouraged as is reading online material relevant to topics being covered. Students are required to read all the materials assigned as scheduled.

2. Project and Project Milestones: Four project-based assignments are given across the semester, each reflecting the development of the project in phases. These project milestones should be submitted via the course Blackboard site. You should feel free to consult with me and others for help, and even consult with your contacts in this area. However, please be sure to submit your own work and cite all external sources properly. For example, students are expected to develop a project proposal, which will be submitted on February 25. Finally, submitted work will be checked by turnitin.com.

3. Exams: Two in-semester exams plus a final exam will be given, covering the material in the readings, discussions and textbook. You are responsible for answers and insights drawn from material that will be covered in the discussions, but may not be in the book.

4. Internet/Blackboard Site: All material including class notes, instructional material, and student assignments will be distributed on the Bentley University Blackboard web site. Grades for assignments and exams will also be posted on the Blackboard web site.

Course Policies

Evaluation

The final course numerical grade will be based on the following components (shown with weights):

In-semester Exams	25%
Project Proposal and Presentation	15%
Class Participation	10%
Final Exam	20%
Final Project, Due May 8	30%
Total	**100%**

The Bentley University Grading System will be used to determine the final letter grade.

Students are to keep track of class standing throughout the semester. It is important to discuss any significant issues with the Instructor **before the end of the course**.

Coursework

Students must read the assigned material before class and be prepared to participate in class discussions. Meaningful class participation and general interest in the course will also influence the final course grade**.** Students are expected to ask and answer questions as well as to offer worthwhile observations on the subject matter under discussion. In addition to participating actively and constructively in class, students must cooperate with team members in any group activities assigned during the term.

Attendance

Students are expected to attend every class. Missed classes will lower your final grade.

Academic Integrity

Bentley University Honor Code

The Bentley University Honor Code formally recognizes the responsibility of students to act in an ethical manner. It expects all students to maintain academic honesty in their own work, recognizing that most students will maintain academic honesty because of their own high standards. The honor code expects students to promote ethical behavior throughout the Bentley University community and to take responsible action when there is a reason to suspect dishonesty.

In addition, the honor code encourages faculty members to foster an atmosphere of mutual trust and respect in and out of the classroom. Faculty are also expected to share the responsibility of maintaining an academically honest environment.

The honor code is not meant to be a cure for all occurrences of academic dishonesty. It does not seek to create a community of informers. Rather, the honor code depends upon the good will to care enough for a friend or a fellow student, even a stranger, to warn the individual to abandon dishonesty for the individual's own sake and that of the community. Thus, the honor code asks all students to share the responsibility of maintaining an honest environment.

The students of Bentley University, in a spirit of mutual trust and fellowship, aware of the values of a true education and the challenge posed by the world, do hereby pledge to accept the responsibility for honorable conduct in all academic activities, to assist one another in maintaining and promoting personal integrity, to abide by the principles set forth in the honor code, and to follow the procedures and observe the policies set forth in the academic integrity system.

The Bentley University Honor Code and this Class

With regard to citation:

- Work done by others should be properly cited. Committing plagiarism is forbidden by the Bentley University Honor code: copying information, ideas, or phrasing of another person without proper acknowledgment of the true source; writing or presenting as if it is your own information, ideas, or phrasing without proper acknowledgment of the true source are all forbidden.
- Using a commercially-prepared paper or research project or submitting for academic credit any work completed by someone else is also forbidden.

With regard to collaboration:

- Homework assignments and the final project are individual efforts. Students may discuss ideas, but the assignments and writing must be done individually.
- Using work done by another student in an earlier semester is not allowed.

You are responsible for seeking clarification from the Instructor for any of the criteria you do not understand.

Learning Disabilities

I adopt the Bentley University commitment to social justice and expect to foster a nurturing learning environment based upon open communication, mutual respect, and non-discrimination. Our University does not discriminate on the basis of race, sex, age, disability, veteran status, religion, sexual orientation, color or national origin. Any suggestions as to how to further such a positive and open environment in this class will be appreciated and given serious consideration. If you are a person with a disability and anticipate needing any type of accommodation in order to participate in this class, please advise me as soon as possible, and make appropriate arrangements with the Office of Disability Services in Jennison (also at 781-891-2004).

Course Schedule

Cybersecurity		
Week / Day	**Topic**	**Assignments**
Week 1 (Jan 18)	Course structure. Introduction to cybersecurity concepts: Security architecture, models, standards (ISO, NIST), attacks, services, policies, mechanisms. Design principles, attack surfaces, trees.	Chapter 1
Week 2 (Jan 22 & 25)	Encryption techniques: Symmetric ciphers, substitution, transposition, rotor machines, steganography.	Chapter 3
Week3 (Jan 29 & Feb 1)	Block ciphers and DES: Block cipher structure, DES encryption and decryption, strength of DES. Block cipher design.	Chapter 4
Week 4 (Feb 5 & 8)	Advanced Encryption Standard (AES): Finite fields, AES structure, transformation functions, key expansion. AES implementation.	Chapter 6

Week 5 (Feb 12 & 15)	Block cipher operation: Multiple encryption and Triple DES, electronic codebook, cipher block chaining, cipher feedback mode, output feedback mode, counter mode (ECB, CBC, CFB, OFB, CTR). XTS-AES for block storage, format-preserving encryption.	Chapter 7
Week 6 (Feb 19 & 22)	Random bit generation and Stream Ciphers: Pseudorandom numbers, generation using a block cipher. Stream ciphers, RC4, truly random numbers.	**Exam 1** Chapter 8
Week 7 (Feb 26 & Mar 1)	Public key cryptography and RSA: Public key cryptosystems, principles and practices, RSA algorithm.	Chapter 9
Week 8 (Mar 12 &15)	Cyptographic hash functions: Applications, examples, requirements and security, hash functions using CBC. Secure hash algorithms, SHA-3.	Chapter 11
Week 9 (Mar 19 & 22)	Digital signatures: Elgamal and Schnorr schemes. NIST, RSA-PSS and Elliptic Curve algorithms.	Chapter 13
Week 10 (Mar 26 & 29)	Key management and distribution: Symmetric key distribution two ways (using symmetric and asymmetric encryption). Distribution of public keys, X.509 certificates, PKI.	Chapter 14 **Exam 2**
Week 11 (Apr 2 & 5)	User authentication: User-authentication principles, using symmetric encryption, Kerberos, using asymmetric encryption. Federated identity, personal identity.	Chapter 15
Week 12 (Apr 9 & 12)	Framework for improving critical infrastructure cybersecurity (NIST): Introduction, history and basics. Proper use, risk self-assessment, framework core.	Supplemental Reading I

Week 13 (Apr 17 & 19)	What's new about cloud computing security? Definition confusion, history, what is not new, what is new, cloud threats, opportunities. Strategic principles for security the Internet of Things (IoT): Overview, principles, practices, guidance.	Supplemental Readings II, III
Week 14 (Apr 23 & 26)	Bitcoin and cryptocurrencies: Classic Bitcoin, Bitcoin transactions and on-chain security, proof of work, alternative consensus, Bitcoin research, stability issues, off-chain security, anonymity, privacy, extensibility.	Supplemental Readings IV, V
Week 15 (Apr 30)	**Final Project Presentations**	
(May 3)	**Final Exam**	
(May 8)	**Final Project Reports**	Submit project final report to blackboard (TurnItIn.com) by 11:59 PM

Appendix C – U.S. National Security Agency Cyber Defense Knowledge Units for Centers of Academic Excellence (NSA, 2018a)

Centers of Academic Excellence in Cyber Defense (CAE-CD)

Foundational KU's			
Cybersecurity Foundations	CSF		
Cybersecurity Principles	CSP		
IT Systems Components	ISC		
Technical Core KUs		**Non-technical Core KUs**	
Basic Cryptography	BCY	Cyber Threats	CTH
Basic Networking	BNW	Cybersecurity Planning and Management	CPM
Basic Scripting and Programming	BSP	Policy, Legal, Ethics, and Compliance	PLE
Network Defense	NDF	Security Program Management	SPM
Operating Systems Concepts	OSC	Security Risk Analysis	SRA
Optional KU's			
Advanced Algorithms	AAL	Intrusion Detection/Prevention Systems	IDS
Advanced Cryptography	ACR	Life-Cycle Security	LCS
Advanced Network Tech. and Protocols	ANT	Linux System Administration	LSA
Algorithms	ALG	Low Level Programming	LLP
Analog Telecommunications	ATC	Media Forensics	MEF
Basic Cyber Operations	BCO	Mobile Technologies	MOT
Cloud Computing	CCO	Network Forensics	NWF
Cyber Crime	CCR	Network Security Administration	NSA
Cybersecurity Ethics	CSE	Network Technology and Protocols	NTP
Data Administration	DBA	Operating Systems Hardening	OSH
Data Structures	DST	Operating Systems Theory	OST
Database Management Systems	DMS	Penetration Testing	PTT
Databases	DAT	Privacy	PRI
Device Forensics	DVF	QA/Functional Testing	QAT
Digital Communications	DCO	Radio Frequency Principles	RFP
Digital Forensics	DFS	Secure Programming Practices	SPP
Embedded Systems	EBS	Software Assurance	SAS
Forensic Accounting	FAC	Software Reverse Engineering	SRE
Formal Methods	FMD	Software Security Analysis	SSA
Fraud Prevention and Management	FPM	Supply Chain Security	SCS
Hardware Reverse Engineering	HRE	Systems Certification and Accreditation	SCA
Hardware/Firmware Security	HFS	Systems Programming	SPG

Host Forensics	HOF	Systems Security Engineering	SSE
IA Architectures	IAA	Virtualization Technologies	VTT
IA Compliance	IAC	Vulnerability Analysis	VLA
IA Standards	IAS	Web Application Security	WAS
Independent/Directed Study/Research	IDR	Windows System Administration	WSA
Industrial Control Systems	ICS	Wireless Sensor Networks	WSN
Introduction to Theory of Computation	ITC		

Appendix D – Cybersecurity Certifications

Comprehensive cybersecurity certifications are currently in development. The organization with the longest track record of offering certifications to security professionals is the International Information System Security Certification Consortium, or $(ISC)^2$. $(ISC)^2$'s most popular certification is the Certified Information Systems Security Professional (CISSP), which, as the name implies, is rooted in information security more so than cybersecurity (Grover, Reinicke, & Cummings, 2015). However, revisions to the CISSP common body of knowledge (CBK) in 2015 and 2018, combined with a work experience requirement, have maintained the relevance and rigor of this certification (Chapple, Stewart, & Gibson, 2018). According to $(ISC)^2$'s web site (https://www.isc2.org) a CISSP candidate today "must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK. Earning a four-year college degree or regional equivalent or an additional credential from the $(ISC)^2$ approved list will satisfy one year of the required experience. Education credit will only satisfy one year of experience." Figure 8 depicts the eight domains in the CISSP CBK as the horizontal stroke of the "T" because of the breadth of knowledge required to obtain this certification.

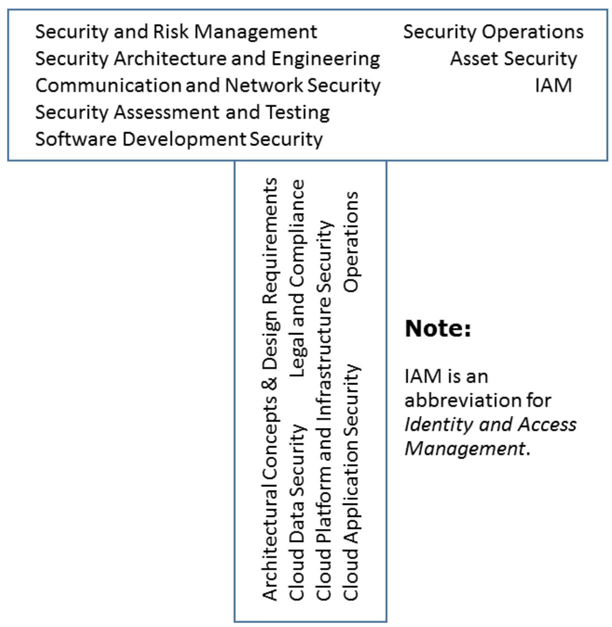


Figure 8: Example of stacked $(ISC)^2$ certifications for cybersecurity professionals. The horizontal stroke of the "T" represents the CISSP. The vertical stroke represents the CCSP.

Although $(ISC)^2$ does not have a certification that carries the cybersecurity name, the CISSP can be supplemented with other certifications, from $(ISC)^2$ or other organizations, e.g., ISACA or CompTIA (Grover, Reinicke, & Cummings, 2015; Hartley, Medlin, & Houlik, 2017; NIST, 2018), to more closely match what a cybersecurity professional might need to know. The vertical stroke of the "T" in Figure 8 shows one such illustrative example by including the six domains covered in the $(ISC)^2$ Cloud Computing Security Professional (O'Hara & Malisow, 2017) common body of knowledge (CCSP CBK). Obtaining the CCSP requires at least three years of work experience in information security and one year in one or more of the six domains shown on the vertical in Figure 8.

The choice of the CCSP in Figure 8 is one of several practical (and marketable) alternatives to demonstrate and certify depth in a specific area (Burley & Bishop, 2017; Wescott & Clark, 2017). As another example, the Information Systems Security Engineering Professional (ISSEP), which is one of three CISSP follow-on certifications, and dubbed the CISSP-ISSEP (Chapple, Stewart, & Gibson, 2018; Ross, McEvilley, & Oren, 2018), is popular among professionals working in the U.S. defense industry. This certification requires at least two years of work experience in one or more of the five domains within the ISSEP common body of knowledge.

In sum, for students that wish to continue their education and training after college, the CISSP and related certifications provide high-quality, cross-industry, and vendor-agnostic certifications that typically will serve them well (Grover, Reinicke, & Cummings, 2015; Hartley, Medlin, & Houlik, 2017; Newhouse, Keith, Scribner, & Witte, 2017; Wescott & Clark, 2017).