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, Massachusetts, USA

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

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, 2003) 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 J. , 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, 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).

Figure 1. Banyan Tree photographed on Oahu, Hawaii

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).

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

ISSN: 2473-3857
v4 n4654

(Parekh & DeLatte, 2018). Furthermore, these foundational principles are strengthened by pairing them with practical examples from cryptography (Stallings, 2017), computer security (Bishop, 2003) 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).

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).

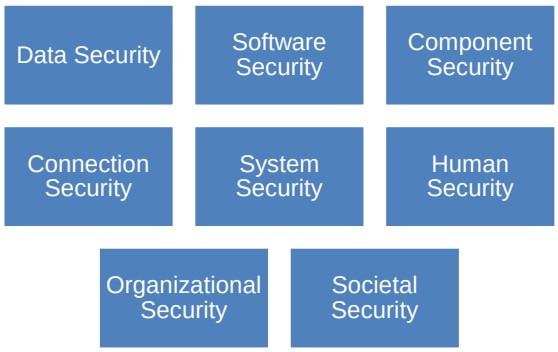

Table 1. Knowledge Areas (KAs) in 2017 ACM, IEEE (CS), etc. JTF Undergraduate Curriculum Guidelines, aka (Burley & Bishop, 2017)

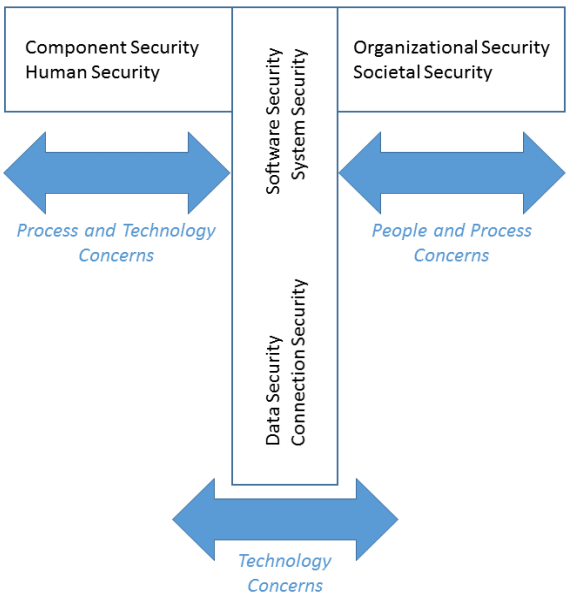

Figure 2. Cybersecurity Knowledge Areas organized in a "T" reflecting holistic, multi-disciplinary breadth and technical depth

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

ISSN: 2473-3857
v4 n4654

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 areas plus five computing disciplines – is recreated from Figure 2 in (Burley & Bishop, 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.

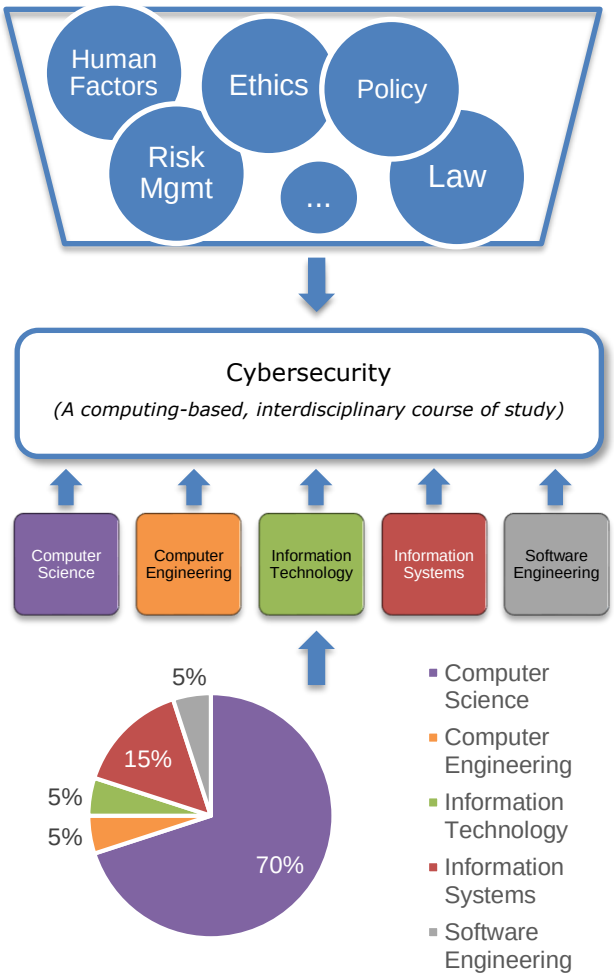

Figure 3. Disciplinary lens for Bentley University CS 401 cybersecurity course

The CS 401 course offered at Bentley 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.

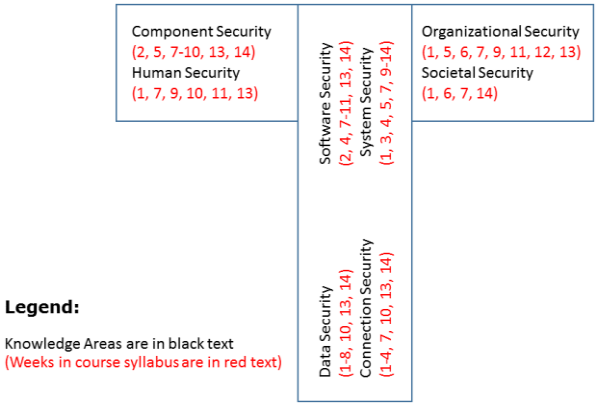

Figure 4: Bentley CS 401 cybersecurity course "T" implementation annotated with week-by-week coverage detailed in Appendix B

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 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.

ISSN: 2473-3857
v4 n4654

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 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.

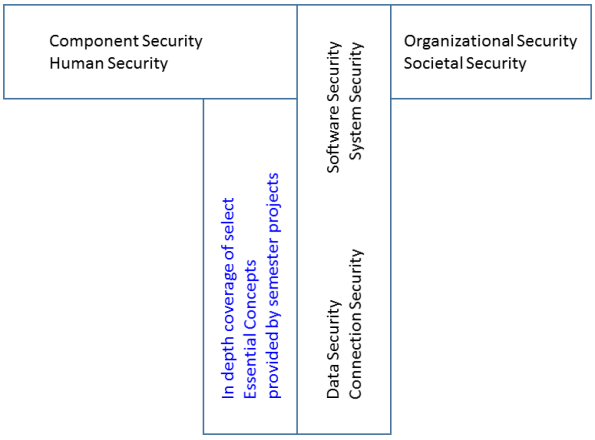

Figure 5. CS 401 cybersecurity course "T" modified by select Essential Concepts from Appendix A

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 reviewed the current usage landscape of security against malware 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 "Gooligan" 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). Yang and Wen's (2017) study focuses on non-technical NSA CAE-CD knowledge and skills in their study, as depicted in Figure 6, because of the connection of these eight Knowledge Units (KUs) to AACSB accreditation.

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).

ISSN: 2473-3857
v4 n4654

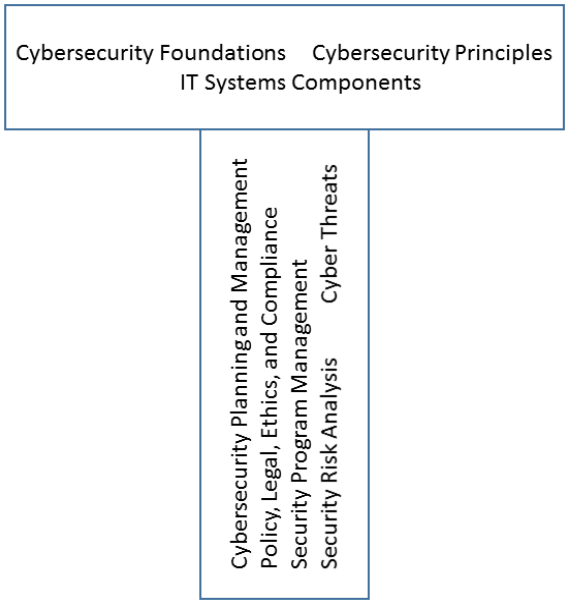

Figure 6. National Security Agency (NSA) Cyber Defense (CD) foundational and non-technical core Knowledge Units (KUs)

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.

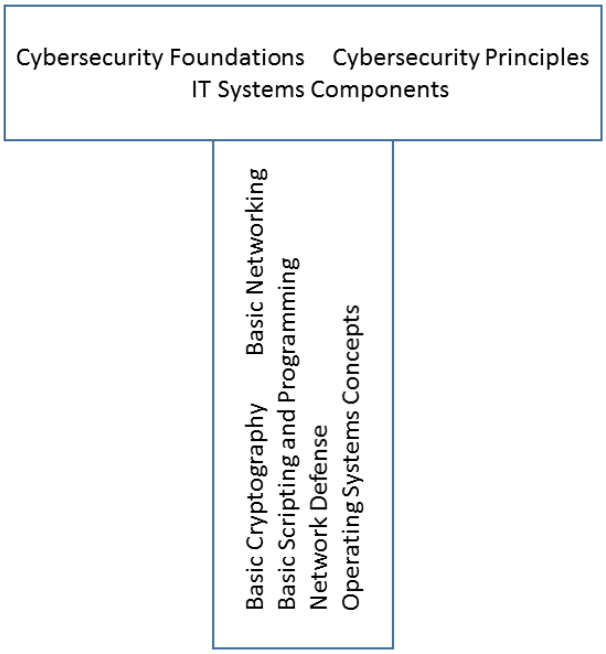

Figure 7. National Security Agency (NSA) Cyber Defense (CD) foundational and technical core KUs

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 Time Magazine's.

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 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 also shown in 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 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 reflects 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 perspective, 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 but provides broader coverage is Bishop (2003) for which a second edition is due out in 2019. Different books might be better for less technical Computer Information Systems majors than McDermott, OConnell and Chen. For example, the texts (Pfleeger & Pfleeger, 2011; 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 J. , 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 all hail from 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 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. (2003). *Computer Security: Art and Science.* 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.

ISSN: 2473-3857
v4 n4654

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	Basic cryptography concepts Digital forensics End-to-end secure communications Data integrity and authentication Information storage security
	Digital Forensics	
	Data Integrity and Authentication	
	Access Control	
	Secure Communication Protocols	
	Cryptanalysis	
	Data Privacy	
	Information Storage Security	
Software Security	Fundamental Principles	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
	Design	
	Implementation	
	Analysis and Testing	
	Deployment and Maintenance	
	Documentation	
	Ethics	
Component Security	Component Design	Vulnerabilities of system components Component lifecycle Secure component design principles Supply chain management security Security testing Reverse engineering
	Component Procurement	
	Component Testing	
	Component Reverse Engineering	
Connection Security	Physical Media	Systems, architecture, models, and standards Physical component interfaces Software component interfaces Connection attacks Transmission attacks
	Physical Interfaces and Connectors	
	Hardware Architecture	
	Distributed Systems Architecture	
	Network Architecture	
	Network Implementations	
	Network Services	
	Network Defense	

ISSN: 2473-3857
v4 n4654

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

ISSN: 2473-3857
v4 n4654

Appendix B – Cybersecurity Course Syllabus

Bentley University – Computer Information Systems Department

CS 401 – Cybersecurity

Spring 2018 Syllabus

Instructor: Z
E-Mail: Z@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 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 Honor Code and this Class

With regard to citation:

- Work done by others should be properly cited. Committing plagiarism is forbidden by the Bentley 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

ISSN: 2473-3857
v4 n4654

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

ISSN: 2473-3857
v4 n4654

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

ISSN: 2473-3857
v4 n4654

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.

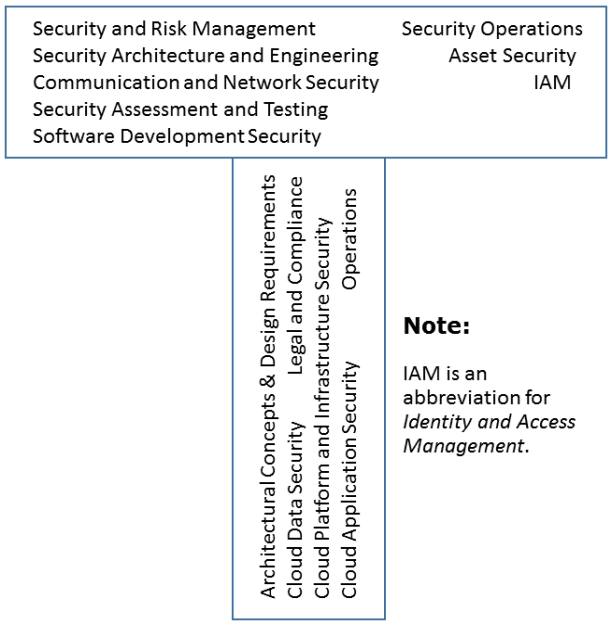

Figure 8: Example of stacked (ISC)^2 certifications for cybersecurity professionals. The horizontal stroke of the "T" represents the CISSP. The vertical stroke represents the CCSP.

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).