Spring 2010

Redesigning the Information Assurance Undergraduate Curriculum at Regis University

Robert L. Winter

Regis University

REDESIGNING THE INFORMATION ASSURANCE UNDERGRADUATE CURRICULUM AT REGIS UNIVERSITY

A THESIS

SUBMITTED ON 18TH OF JUNE, 2010

TO THE DEPARTMENT OF INFORMATION ASSURANCE

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

INFORMATION ASSURANCE

BY

Robert L Winter

APPROVALS

D. M. Likarish

Daniel M. Likarish, Thesis Advisor

Douglas I. Hart

Douglas I. Hart

Richard L. Blumenthal

Abstract

When Regis University created the eSecurity curriculum in 2003, the lessons were pertinent to the then-current threats. Although the curriculum has slightly changed since then, the courses needed a major facelift to meet the ever changing cyber threats. The question of can Information Assurance courses at Regis University be refreshed to include virtual labs so they are based on ethical standards will be answered in this paper. Utilizing the Design Science methodology and incorporating Bloom's Taxonomy and the Jesuit educational approach, curriculum was identified and developed for the classroom and online students. By working with the Regis Distance Learning department, the thesis project was submitted for publication as part of the Regis Computer Networking courses.

Acknowledgements

I would like first and foremost to thank my wife, Erin, for all of her patience during those nights when my head did not hit the pillow until the wee hours of the morning and for allowing me to go on those long bicycle rides to clear my thesis thoughts. To my children for all of those times I was studying instead of playing, trethandi! I would also like to thank Professor Kim Herfurt for being a wonderful friend and my trusted advisor and to Professor Ron Sander for giving me the freedom to express things in a creative manner to achieve wonderful end results. Many hearty thanks also go to my other professors that have assisted in my growth at Regis. Finally, to my family, friends, teachers, and co-workers who inspired me to concentrate on Information Security, I am eternally in debted as I have an inspiring hobby that doubles as a strong career. Not too many people can say this, so I consider myself quite lucky.

Table of Contents

List of Figures

Chapter 1 - Introduction

Since their inception at Regis University in 2003, the eSecurity courses have had a strong following but have not been revised to reflect changes in technology. In 2009, the Regis administration dictated a review of these courses to determine what worked, what needed improvement, and how to offer online courses in an ethically responsible manner. Online students can reside anywhere in the world and teaching online students can be difficult due to the physical distance between the educator and the student. When those students are full-time working adults who are learning hacking techniques, ethical and trust factors become paramount. As countries have created their own cyber armies to defend and attack (Miles, 2009), it may be difficult to discern the ultimate intentions of online students. Due to this concern, the ethical use of the Information Assurance curriculum has become extremely important. While ethics were taught in the previous design, it is now paramount to have ethics integrated into each and every topic of these courses. The goal of this project is to recreate the Information Assurance curriculum with an online component and virtual labs that can be ethically taught.

1.1 - Project Proposal

Shortly after horrendous events on September 11, 2001, the United States Air Force Academy in Colorado Springs, Colorado, approached Regis University to develop and teach computer security courses. The first of these courses were taught in mid-2003 to students at the campus in Colorado Springs and the Lowell campus in Denver. The courses offered those who wanted to learn how to protect their data with the foundational knowledge. Since the creation of the courses in 2003, the curriculum was not significantly altered.

Stamos Karamouzis, the dean for Regis' School of Computer and Information Sciences, stated in a presentation during the summer of 2009 that he would like Colorado and, in particular Regis, to be the center of Information Assurance for the region. The courses were already due for a redesign as the books and material for most of the program had become outdated and the bookstore was having difficulty obtaining out-of-print copies. The transient nature of the labs dictated they had to be rebuilt every time a new class was offered and, over time, the equipment had become antiquated. As approximately forty percent of the undergraduate student population accesses online courses, financial motivation helped to move the courses to the online format (U.S. News, 2009). A contributing factor to the increase in attendance for the security courses is related to the computer networking degree plan requirement for all students. Since all students working toward a degree in Computer Networking are required to complete CN460 and CN461 (Regis University, 2010), it is necessary to have these courses online from both a monetary and educational standpoint. All of these requirements made the revisions a priority.

The Regis Computer Networking students tend to be working adults and education techniques are different from traditional students (Jones, 2003). As the learning techniques need to be different, the courses will be developed using the Design Science methodology, Bloom's Taxonomy, and the Jesuit educational approach. Interactive labs will give the students a chance to reinforce their knowledge through edu-tainment. Edu-tainment can be described as the presentation of educational learning topics in a fun and entertaining format. For adult students, this teaching method can be critical for memory retention. Using this learning process, the mature learner will be able to demonstrate acquired knowledge in Information Assurance.

1.2 - Scope of Project

This project is limited to the redesign of CN460 (Fundamentals of eSecurity) and CN461 (Security Breaches) courses. These two courses form the foundation for the Information Assurance undergraduate program. With the inclusion of these courses in the Computer Networking degree plan in 2008, the students are formally exposed to the value of securing their environment's data. This project consists of the creation of the curriculum and all associated coursework and labs. Any courses and course development, other than CN460 and CN461, are outside the scope of this document.

1.3 - Project Discussion Questions

At the onset of this project, there were two questions that needed to be answered: What constitutes computer ethics and what knowledge should the student have to attend these courses? According to the $(ISC)^2$ Second Canon of Ethics, a computer security professional should "act honorably, honestly, justly, responsibly, and legally" ($(ISC)^2$, 2009). As a participant in the Regis University Information Assurance courses, the student should strive to do what is morally correct both in the eyes of society and God. From the scholarly perspective, the student should not test the security on systems they do not own, nor should they test it, without explicit permission from the appropriate level. There is no gray area in security. This simple, yet highly critical ethical practice, is often overlooked.

The students should have attended the entry level computer networking courses offered by Regis University, including CN301 - Networking Technologies and Fundamentals; CN311 - Systems Architecture; and CN316 - Network Architecture. These courses are critical to the students before they move their education to the 400-level (senior level) courses. Without the knowledge obtained through these introductory courses, or similar courses offered at other academic institutions, comprehension of the learning topics will be difficult. Students who ignore the prerequisites could potentially be setting themselves up for failure in the Information Assurance curriculum. To ensure the highest level of success prior to entering the CN460 course, the students will be challenged by a self-assessment exam, created as part of the redesign, to help identify potential weaknesses and offer remediation steps. Having prerequisite knowledge will make the courses more valuable to the students and the discussions more productive.

1.4 - Summary

By attending the Regis CN 460 and CN 461 courses, as well as other courses offered by the Regis University Computer Networking curriculum, the students will learn how to mitigate computer-based threats. Whether the student becomes a security engineer, an expert in Information Technology, or just a user of the latest technological trend, their education will help to protect the assets and data under their charge. Using techniques designed to engage the adult student, these courses are designed to foster thought provoking learning and eliminate the traditional lecture and reading format of previous classes. As people become more knowledgeable about the world around them and the data they possess, they will be able to better secure themselves and those around them.

Chapter 2 - Review of Literature and Research

In order to have a full background and appreciation of computer security, a wide variety of resources were selected by the thesis author. This selection provided an appropriate level of knowledge and substance for the creation of these courses. A combination of text-books and online resources provided a foundation for the learning topics.

2.1 - Course Specific Literature and Research

In June 2008, Regis University formed a curriculum development committee to redesign the computer networking courses. One of the tasks the committee completed was a mapping for all major learning concepts (See Appendix A). Students, advisors, facilitators, and course developers can use this mapping to visualize course prerequisites and understand why they are required as foundations of the security curriculum. As shown in Appendix A, every course redesigned has been added to the mapping. If an advanced course lacked an introductory component, the necessary foundation was added to the corresponding lower level course. Without this foundation, the students will miss critical pieces while attempting to secure their environments. By having every learning topic map to another topic or topics, the students will have a more cohesive learning process.

When deciding what to include in the security curriculum, the thesis author determined, based off of research and first-hand knowledge, that a foundation in networking was required. Students come into Regis University with a wide array of knowledge. Some of the students have taken networking courses, while others may be new to the field. To be an effective Information Technology security professional, one needs to understand how Information Technology on a computer network functions. Several frameworks and learning sources were evaluated for their educational usefulness. The decision was made to follow the United States Department of Defense Directive 8570.1 (DoD 8570), as it applied appropriately to the requirements. Regis University has been recognized as a United States National Security Agency Center of Academic Excellence in Information Assurance, so this too fits with the directive. The government regulation requires a minimum amount of applied knowledge demonstrated by obtaining one or more specified certifications as listed in the directive. Within the Information Security industry, the single most challenging certification designated by the DoD 8570.1 order is the $(ISC)^2$ Certified Information Systems Security Professional, abbreviated as CISSP, certification. The core body of knowledge (CBK) behind the certification consists of ten security domains. Each domain has a unique area of focus. The material from each domain can overlap another, and the knowledge obtained in all ten domains is essential to proficiency as a working security professional. Through this foundation, a student will be provided with have the skills and ethics to succeed in the subsequent courses at Regis and in their career.

Reviewing course work provided by other academic institutions was performed. The City College of San Francisco's Dr. Sam Bowne offers courses using hands-on labs. These courses have strong classroom attendance but do not require the academic writing expected for Regis students. In reviewing the coursework from Georgetown University, Colorado State University, and Western Connecticut State University, the topics focus more on the programming aspects of computer security than the networking aspects. These curriculums did help to provide a review for potential course topics but due to the uniqueness of the Regis education and as this is for the Computer Networking degree, additional information was required.

The next step was to evaluate the books. Within the CISSP world and the information security industry, there are two books that are consistently recommended for study: The *CISSP All-in-One Exam Guide* by Shon Harris and the *Official (ISC)*^{2} *Guide to the CISSP CBK* by Harold Tipton. Of the two guides, the book by Shon Harris provided a well-written guide that is easier for students to understand key concepts. The *Official (ISC)*^{2} *Guide to the CISSP CBK*, while packed with valuable information and a superb resource for reference, does not read smoothly from cover to cover. The decision was made to use the *CISSP All-in-One Exam Guide*. For supplementary material regarding the risk of computing in our daily lives, *Security for Ubiquitous Computing* by Frank Stajano was selected. As more and more mobile devices are network-enabled, the likelihood for data leakage or a critical failure through ubiquitous devices increases. These personal-use devices may lack attention to security during manufacture, such as Vodafone's distribution of a line of their cell phones complete with malware (Mills, 2010), and can have devastating consequences to networks. Other literature reviewed for the courses was not selected as it did not properly address the topic or lacked depth. The *CISSP Guide to Security Essentials* by Peter Gregory is a good review manual but does not promote critical thinking or apply knowledge. Outside of printed learning material, audio and video provided by web-based security publications such as SearchSecurity.com give the students a secondary source of information. Computer testing simulation software vendors, Transcender and Self Test Software, help to reinforce the knowledge, but these sources were not included as the knowledge focused too much on the exam and not enough on building the required fundamental knowledge. For students who want to challenge their knowledge on each of the ten domains, the CCCure.org site, run by Clement Dupuis, does an excellent job with a quiz bank and does it at no cost. Unlike costly simulation quizzes, this site provides students an economical way to find weaknesses in their learning and learn to address them. Videos were also reviewed such as *The Shon Harris CISSP Video Seminar* series. This provided the security topics with supplementary learning methods. However, the cost does not always justify the benefit. Free videos such as those published by the BlackHat, DefCon, SnowFROC, and ShmooCon security conferences do offer knowledge that can be downloaded, but students need to remember ethics are not always presented. For the foundation security courses, two sets of videos were selected. A video called *Cyber War*, published under PBS's Frontline series, offers an introduction into the world of computer-based attacks. For students new to the field, this is an excellent video to set the stage for critical learning. For physical security, two short *Tiger Team* videos published by TruTV do focus on physical security. The students are introduced to the methodology of attacks, both physical and logical. By using a combination of printed literature, videos, web-based simulations, and live CDs, the courses met the requirement of providing the students with an edu-taining experience.

2.2 - Known and Unknown About Project

With the (ISC)^2 Core Body of Knowledge (CBK) selected, the ten domains had to be distributed across two, eight-week sessions with concern for the sequence of the learning topics. The anticipated student workload for each domain was evaluated to ensure that students had enough time for the weekly learning topic while not extending the duration for the domain. The readings were intentionally limited to less than one-hundred pages per week when possible. The labs were focused on specific and measurable learning topics, and written assignments were constructed so that students could demonstrate acquired knowledge. Once the basis for each week had been decided upon, the week-by-week schedule was laid out.

2.3 - Project Contribution to the Field

While the field of information assurance is still in its youth, there are plenty of information sources available. Knowledge of the topics can be obtained through sources on the Internet or through courses taken through private, non-academic training providers. Academically there are a number of National Security Agency Centers of Excellence in Information Assurance, but what separates Regis University from the rest of the certified academic institutions is the Jesuit method of education. Through self-reflection, group discussion, and hands-on learning, the student will be exposed to a wealth of value laden information organized in a logical and ethical format.

In revising these courses, many things needed to be addressed from a teaching perspective to reach the view Dean Karamouzis has envisioned. Regis University is not a technical or vocational school, so the classes cannot be created with a plethora of physical labs and wrapped in shiny quick packages. The labs also need to provide immediate value to students in their daytime jobs so they can demonstrate their increased knowledge to their employers and themselves. By redesigning these courses, students will be able to receive an education that will meet the vision.

Most students are working adults with families. A typical adult student puts in a minimum of forty plus hours a week for their job prior to switching gears to focus on school. Many of these students need more than just lectures to hold their attention into the evening hours. By involving Design Science methodology where the experiences from the students' jobs can directly enhance the learning, the curriculum can capture the students' interests. By meeting the needs of the students, while meeting Regis's rigorous academic needs and expectations, the security courses were redesigned using 'edu-tainment'. The curriculum developers define edu-tainment as the ability to take traditional university material and present the material with new technology and entertainment-style techniques.

To reach the goal of edu-tainment and provide a fresh perspective to the students, several new technology changes were introduced. Live Linux CDs with labs are now a mainstay within the courses. A live CD contains a fully functional operating system along with the necessary application files for the student. The disk provides a lab on a self-contained disk the student can use on a Regis computer or on their own personal computer. For the security courses, live CDs from information security community projects such as the Open Web Application Security Project (OWASP) LabRat and the Heorot De-Ice Penetration disks were selected. The advantages to using live CDs are numerous. The students are expected to download the compressed files before the first class and alternative options have been planned for students experiencing technical difficulties. If the student has the required technology but cannot get the labs to function correctly, the labs will be burned to disk and sent to the student through the United States Postal Service. All students are able to experience the same labs regardless of their location and the experience is immediate. If a student's computer was purchased in the last several years, they have the ability to run the lab natively on their hardware or inside a virtualization application such as VMWare, Parallels, VirtualPC, and VirtualBox. A virtualization application allows the computer to operate a simulated or virtual operating system separate from the host system. If the student has an older computer, a virtualization lab has been set up so the students can log into the Regis Academic Research Network (ARNe) and run the labs over a VMWare ESX server. The undergraduate program will be integrating some of the labs with Second Life. Second Life is designed by Lindon Labs as a virtual world. People can interact with each other in an online graphical environment without leaving their physical location. From the Regis perspective, students can create their own personalized computer representation of themselves, called an avatar, and visit the Regis University School of Computer and Information Sciences (SCIS) site within Second Life. The advantage of labs like Second Life would be for students who have never previously viewed a computer data center. The student can perform a full physical site survey where they can identify potential security risks, watch educational training videos uploaded by the facilitators, and can visually interact with other students. These technologies bring students into the Regis community and allow them to interact with one another regardless of distance. The redesigned program will help to meet the edu-tainment goal where real life knowledge can be gained rapidly while the foundations of the technology are reinforced for the working professional.

Chapter Three - Methodology

The courses incorporated a combination of Design Science, Bloom's Taxonomy, and Jesuit educational approach to maximize the students' learning experience. By using these educational approaches along with the course material, each learning topic was reviewed through the different phases of analysis, design, implementation, testing, and maintenance. Due to the deadline date required for the curriculum guides and the thesis document, the testing and maintenance phases were minimized. Additional work outside of this document will be conducted to ensure these phases are addressed in a satisfactory manner.

3.1 - Analysis

Design Science was used in the course creation process. According to R. Buckminster Fuller, a pioneer in the Design Science field, "Design Science is a problem solving approach which entails a rigorous, systematic study of the deliberate ordering of the components in our Universe. Fuller believed that this study needs to be comprehensive in order to gain a global perspective when pursuing solutions to problems humanity is facing" (Buckminster Fuller Institute, 2010). In each of these individual courses, design science was used to integrate and explore comprehensive learning.

Care was also taken to utilize Bloom's Taxonomy. For each of the six different cognitive levels of learning, each level builds off the previous level until mastery has been accomplished (Slatta, 2007). The lowest level, remembering, allows the student to recall the material without full comprehension. In the Information Assurance courses, this is accomplished through activities such as definition memorization and observing videos. The second level of Bloom's Taxonomy is understanding the material, such as utilizing tables in a student's presentation.

Applying one's knowledge is the third level. A student able to differentiate between a symmetric and asymmetric cryptographic algorithm would fall into this category. When students are able to dissect the material into a concept's most basic parts, they have reached the analysis phase.   For the Information Assurance student, this is demonstrated through the critical thinking required at the end of each learning topic. Being able to defend one's position on a subject moves the student into the evaluation phase. Students are expected to critique each other's positions, but also be able to constructively argue, defend, and validate their own thoughts and ideas. The final level of learning in the Bloom's Taxonomy is creating material. Students are not expected to run through a series of multiple choice questions and simply regurgitate information. Through written demonstrations, the students will be exhibiting their knowledge in a coherent and cohesive manner and be able to evaluate their ideas. Through presentations, the full range of Bloom's Taxonomy can be accomplished. Figure 3.1 illustrates how the student can move from a lower order of thinking skills to a higher order.

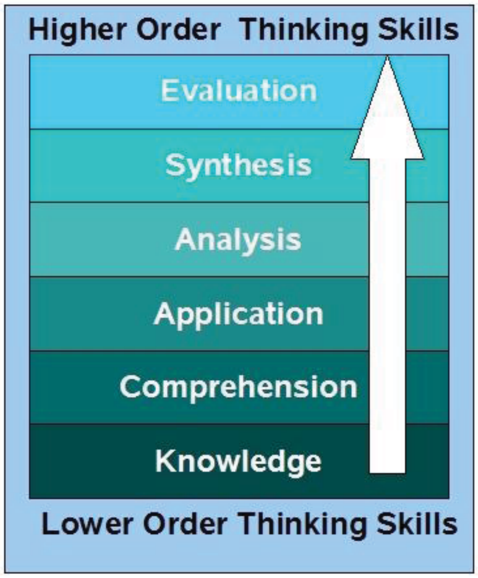

Figure 3.1

In combining the Bloom's Taxonomy with the Jesuit educational approach, the instructors help the students achieve the required results. “Since the time they launched their first school in 1548, the Jesuits have believed that a high quality education is the best path to meaningful lives of leadership and service” (Kolvenbach, 2005). The Jesuit method of education reinforces critical consciousness and encourages students to strive to their fullest potential. Through reflection and group discussions, the students will be able to explore, question, and comprehend their world in a broader perspective and apply these concepts.

3.2 - Design

Information security students need to understand threats to their environments, how they are initiated, and how to mitigate the associated risks. Ignorance can no longer be accepted as an excuse. Learning these techniques is critical. Traditionally the Regis courses were only offered in a classroom and a single faculty member was able to observe the progress and actions of the students. Now that these courses are offered online, an assessment of the students’ ethical intentions is much more difficult to make. While ethics were taught in the previous design, it is now paramount to integrate ethics into each topic taught during these courses. During the research of this topic, several other colleges and universities around the United States such as Georgetown University, the City College of San Francisco, and Carnegie Mellon University have an ethics statement for their information security programs. The students are required to read, acknowledge, and sign an ethics statement at the beginning of each course to ensure the student fully understands the information they will be learning has both good and bad aspects. During the design of the Regis courses, an ethics statement has been included to make sure the students remain on the ethical side of information security learning. Understanding how environments are threatened is important but learning should always be done in an ethical manner.

3.3 - Implementation

For the Implementation Phase, each learning topic was reviewed and assigned to one of the two courses as described below in 3.3.1 - CN460 and 3.3.2 - CN461. These courses are connected as a series where the knowledge is built in a sequential order. The students are expected to attend CN460 prior to CN461. The full curriculum guides for CN460 and CN461 have been accepted by the Regis Distance Learning department and could not be presented in this paper due to the intellectual property nature of the material.

3.3.1 - CN460

During the first week of the Fundamentals of e-Security course (CN 460), a basic understanding of security trends and information security is addressed. Information Security changes rapidly in response to newly developed attacks and the changing requirements of data owners. The security trends topic must be constantly re-evaluated to keep it up to date. Today's engineers need to know where their data is located within the environment and all of the potential attack vectors in and connected to the network. The knowledge addressed during this week's topic is focused on those aspects. Inquisitive hackers and malicious crackers (hackers with a criminal characteristic) are constantly evolving their attack methods, and so must the successful information security professional. The great Chinese military strategist, Sun Tzu, stated “Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning and losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.” (Tzu, & Griffith, 2005). Reinforcing this basic level of network knowledge sets the foundation for the rest of the security topics.

Risk management is a cornerstone of information security. When a security professional evaluates what he should secure on their network, he calculates the risk of loss associated with the value of the data he is protecting. The student learns his role as an information security professional versus the role of executive management in dealing with risk management. Once vulnerabilities and threats have been identified and presented to management in an unbiased format, management can mitigate the risk, transfer it, or accept the risk. There are times when the value of the information does not warrant the associated costs of the protection and management simply accepts the risk however students are taught that ignoring the risk is not an acceptable option. During this second week, a review of the PBS *Cyber War* video will reinforce the talking points and provide points for interactive discussion. Since information security deals with risk management, this is a perfect core learning topic.

Physical security is an easy topic for students to learn due to the real-world experience conceptualizing the information. If an attacker is able to obtain physical access to your data, the information is no longer considered "your data". Threats within this domain can come from data stored on portable media, natural disasters, or directed attacks at the physical infrastructure. During this third week, students will watch the two *Tiger Team* videos, which emphasize that no matter how securely you think you have protected data, the smallest omission in physical security can result in an enormous loss. Care should be taken by the information security professional not to overlook physical security.

Week four of CN 460 introduces the students to the history of ubiquitous computing. Network-enabled devices have made our lives easier, but have also exposed networks to increased risk. Improving business workflow is a positive aspect of network-enabled devices. A hospital in the United Kingdom, for example, has integrated technology into their workflow process, where strategically placed monitoring devices can detect a patient being wheeled to the operating room. An elevator en route to the patient's destination can drop off non-critical passengers so it is positioned on the floor and empty when the patient arrives. The ubiquity of this technology can improve business workflow and patient care. On the negative side of network-enabled devices, cellular phones with global positioning systems (GPS) can assist an individual to find an address, but other entities can also gather that data to know that person's exact location. This has been known to occur with large marketing corporations who collect and sell this information, but it can also be used for more nefarious purposes. Websites have been created on the Internet to collect data from social networking sites to show when people are out of town and their houses are prime for theft (Cluley, 2010). These sites are using information predominantly published by the home owners who do not consider the full ramifications of their actions or their loss of privacy. General Motors' offers the OnStar service to assist stranded consumers who lock the keys in the car or disable engines of vehicles pursued by law enforcement officers. If a malicious attacker could gain control to this type of system, the effects could be devastating. As the students examine and understand ubiquitous computing, they will have a better appreciation for the risks that these advances in technology provide.

Access control of their computer environment is the topic for weeks five and six. When attempting to control what a particular person or subject can access in regards to a specific object, access control is involved. Confidentiality, integrity, and availability are considerations for security engineers for when securing an environment. The students will explore access control methods and models to help better understand how to secure their environments. By controlling access to systems, whether physical or logical, and preventing the unauthorized disclosure, alteration, and destruction of data helps to ensure security to the environment can be increased.

To close out the first eight week session of the security courses, the students apply the knowledge learned to security architecture and design. While not all students may want to become an information security architect, understanding how computer hardware and operating system architecture function will provide the students the ability to protect these systems. On weeks seven and eight, the students will learn to create a security plan using the knowledge acquired during the course. The written paper and required presentation fulfill Regis University's focus on 'learners becoming leaders'. Classrooms are now borderless, so remote students are expected to make presentations as well. Remote students will be able to make a presentation using a webcam, cell phone, or other electronic devices. For those without the necessary video technology, digital presentation software applications such as Microsoft PowerPoint and Apple Keynote can provide a voiceover with the built in microphone on a laptop or an external microphone with a desktop. By adding a face or voice to the course, the students are able to help overcome the electronic barriers created by online classes and achieve a more personal interaction. The knowledge learned over the first eight weeks will allow the students to continue to the next course, CN 461, and to properly assess the security of their daily activities as well.

3.3.2 - CN461

The second in the series of information security courses offered by Regis University, CN 461 - Security Breaches, continues the CISSP CBK by examining the second set of five domains. As this course builds upon the skills acquired during the first course, admittance into this class without CN 460 as a prerequisite is strongly discouraged. The first of the domains examined is telecommunications and network security. Topics covered include the OSI model, protocols, and network design in depth. Due to the mountain of knowledge introduced in this domain, the curriculum is spread over two weeks. This domain is probably one of the best known for anyone currently working on the infrastructure side of Information Technology, but most students are surprised at what they do not know and the amount of information.

The second two-week block for CN 461 focuses on cryptography. Students learn that the secret of strong cryptography is not in the secrecy of the algorithm but rather in the safeguard of the key. Given enough time and effort, any algorithm can be cracked, but those algorithms which have been vetted for flaws and corrected tend to be far more secure. Computer software and hardware vendors try to secure the data using their own proprietary encryption algorithm. During the class, the students will examine the different cryptographic components and their relationship. A cryptography lab is included with this topic, allowing the students to try different algorithms on blocks of text so they can visually observe the results. Having an understanding of cryptographic algorithms, their strengths and weaknesses, and the attacks and mitigating techniques will only make security professionals stronger in their abilities to defend their environments.

CN 461's Week 5 moves into the rapidly developing world of application security. For most students in the Computer Networking degree, this topic is difficult to understand. Most students have focused on the bits and bytes of the network, rather than the topmost layers of the ISO OSI. The fifth through seventh layers of the OSI model are where many of the current attacks are originating. While the security industry has slowly locked down the lower layers, poor application development practices have increased the attacks on this domain. As demonstrated by the rise of attacks on vendors such as Adobe, application security needs some serious attention. Utilizing the OWASP LabRat lab, the students learn to simulate attacks and understand mitigation techniques in a safe, isolated manner. Since applications can be cross platform installed on a huge number of computers, attacks are moving to this format. Learning techniques to prevent these attacks are vital to future security experts.

When working with security, the operational aspect is required to keep the highest service levels while reducing costs. The learning topic for week six focuses on operational security. Businesses pay a lot of money for technology solutions to assist with their workflow processes. Unfortunately, security is not always at the forefront of the process and that can lead to negative consequences. Operations security can assist the department by controlling access to applications, reviewing logs, monitoring activity, and performing audits. Keeping the systems free from attacks is paramount. By focusing on the day-to-day activities, the students learn how to keep the business functional and secure.

The seventh week covers the catastrophic domain of business continuity planning and disaster recovery. After September 11th, several companies who were established in the World Trade Center buildings never opened their doors again. Some of the corporations in the New Orleans area did not adequately prepare for such a disastrous hurricane as Katrina. Organizations need to be prepared for a disaster whether implemented by a terrorist or through the work of Mother Nature. Preparations, however, do not stop once the disaster recovery and business continuity plans have been created. These plans should be continually tested and retested to validate and improve upon the strategies. Hardware and software applications are continuously updated and contingency plans must reflect the changes in infrastructure within an organization. By taking steps to prepare for events outside the control of the company, the security engineer can help make sure the business thrives no matter what happens.

The last domain covered during CN 461 is legal situations and associated investigation processes. Thieves steal, con artists scam, vandals deface, and criminals commit crimes. Thirty years ago these events would have occurred predominantly in the physical world, but today they can also be found in abundance in the virtual world. Knowing what motivates these attackers and the appropriate response supplies the security professional with the tools to identify, investigate, and pursue justice for the data owners. When an investigator fights cybercrime, they are only as good as their ethics. For an investigator, a highly developed sense of ethics is critical to a lasting, long term reputation. A strong moral code of conduct is not an option if one intends to remain in Information Assurance. The students will create a business continuity plan for the fictitious corporation, WigIT, used throughout the two courses. The associated academic paper is due week seven and the presentation will be due during week eight. Students are expected to present their final project for CN 461 in digital format regardless of their locale using skills learned during the CN 460 final presentation. When the students have concluded this week, they will be well positioned to both participate in the information security community and to attempt the CISSP exam.

3.4 - Testing

Based off of discussions with the Regis Distance Learning department, the first time the redesigned CN460 and CN461 courses will be offered will be during the Fall 2010 semester. During the creation of the updated courses and associate coursework, the project had an iterative review process. Initial responses and critical feedback was solicited and received by Computer Networking department professors Kim Herfurt and Ron Sanders. The change cycle was repeated until all ambiguities were eliminated. At that point, the material was submitted to the Regis University Distance Learning department. One of their instructional designers, Yvonne

Bogard, increased the scrutiny of the material through her own iterative review process. All changes were made and the final curriculum material was submitted to the web team. Ensuring the evaluation phase of Design Science was effectively used, the descriptive method was used to appraise the project. The scenario portion of the descriptive method was used to evaluate how students may react to the coursework and material. Based off of the feedback provided by the reviewers of the artifacts and the inclusion of the material into the CN460 and CN461 courses as the primary educational material, it is believed the project was successful in its effort. Due to the first time the CN460 and CN461 courses will be offered with the updated curriculum will be Fall 2010, a review for student feedback should be performed to assess the clarity and fluidity of the work.

Since student-based feedback, testing, and maintenance are not possible in the scope of this thesis, the author of the curriculum has committed to reviewing the student feedback and to perform modifications. As with all courses, CN460 and CN461 need to be assessed once the classroom and online sessions have concluded. From a teaching perspective, the facilitator will need to analyze each learning topic, record and document what worked, what did not, what the student understood, and what topics they had difficulties learning. In addition to the teacher's observations, student feedback is required for the testing phase through formal and informal channels. The end of the course survey allows the course developers, facilitators, and academic administrative staff to review the redesigned curriculum against historical data. Through the constant interaction with the students, an informal survey will allow for students to suggest ways for the topics to function smoother or more logically. Once this information has been aggregated, the course developers should review the data to determine areas of additional improvement. The outcome will allow for the maintenance phase to occur and for the curriculum to be further enhanced.

3.5 - Maintenance

The courses should be examined and updated, at a minimum, every two years. As technology changes, so do the attacks. Care should be given to ensure the information provided in these courses is kept relevant while adhering to the ethical and edu-tainment aspects. These courses may also have to be re-examined if any of the learning materials change so that students may obtain the necessary supplies. As part of the maintenance phase, the labs should be moved from live CDs to an environment supported by Regis to limit technical difficulties that may be experienced by the students. While the live CDs give the students the freedom to complete the virtual labs anywhere, the differences in student computers can result in different academic experiences. To be at the forefront of Information Assurance education is an admirable goal, but one that requires commitment and funding from the University and Information Assurance department to ensure the curriculum is up-to-date and fully functional.

Chapter 4 - Project Analysis and Results

Having participated in previous course revisions at Regis University, the thesis author understood the expectations. In an effort to improve, these expectations were elevated to the next level which definitely presented a challenge. It is critical for both Regis and this program to keep moving forward and enhancing the curriculum.

4.1 - Project Learning Experience

These courses provided a wonderful opportunity to apply the author's career knowledge and passion and package it into a better Regis program. CN460 and CN461 will provide students with a strong foundation for information security. Using multimedia techniques for edu-tainment learning, the courses have integrated videos, games, labs that can function as standalone modules, and the online experience, Second Life. By adding more than lecture to the courses, the students will experience a more active learning environment. Thanks in part to the curriculum development, the thesis author was able to attempt and pass the (ISC)^2 CISSP exam in December 2009. While the author will be leaving his life as an academic student and looking forward to the next chapters of his life, he knows the redesigned courses have met the challenge.

4.2 - Project Enhancements

There are two areas for improvement and enhancement of these courses. The first one is technical. While care was taken to create labs where live CDs can be used, Regis University should take steps to enhance its infrastructure and invest in this curriculum. Architecture discussions with Professors Barnes, Moore, Herfurt, and Sander were conducted during the research to decide what level of technology Regis could offer. An environment consisting of a VMWare portal for both classroom and online-based students should be procured using currently top technology and maintained by a staff other than graduate students. A lack of this environment will prohibit Regis University from reaching its goal of becoming a top Information Assurance school, as other schools in the region surpass it. The second area is the knowledge and expectations of the students. The revised curriculum may help to improve the situation, but Regis should raise, not lower, its expectations of students. This is the Jesuit way and should be the Regis way.

4.3 - Goal Obtainment

As the author reflected on whether the Information Assurance courses could be refreshed to include virtual labs so they are based on ethical standards to both classroom and online-based students, the goal was obtained. Regis University now has both CN460 and CN461 with their Distance Learning designers in the final review stage. These courses will be offered during the Fall 2010 semester. The testing and maintenance phases will be critical to the success of the courses, but the philosophy to improve these courses has been implemented. These courses will move Regis University into a position where online students can obtain the same educational level as their classroom-based counterparts without compromising the ethical standing of either the school or the student.

4.4 - Future Additional Courses

While the first two courses will provide a solid foundation for the students, they are definitely not the only security-focused classes for the Regis University Computer Networking degree plan. Future courses are in the works to expand the undergraduate security curriculum. These expansions will include a penetration testing course and computer forensics. The penetration testing course will focus heavily on ethics while the students learn about methods to breach the security system and ways to reduce the exposure. Computer forensic analysts are needed both in the commercial and government ranks. A network and computer forensics course will cover the topic touched on by the CN461. While ethics should be a component of any security program, the judicial and legislative branches of the government pass new laws every day. For those not familiar with the laws, the associated violations can be costly. A course specifically designed around the analysis and interpretation of ethics and law will posture the security professional above their peers. For those who want to explore the inter-workings of cryptography, a course on this subject will be created. As use of wireless technology continues to grow, a Wireless Network Security course is planned for future curricula. Other courses may be included in the future, but the knowledge by the students will produce alumni that will meet and hopefully exceed Dean Karamouzis' desire to be the center of Information Assurance for the Rocky Mountain region.

4.5 - Summary

The redesign of CN460 and CN461 will provide Regis students with an up-to-date Information Assurance education. Utilizing edu-tainment techniques to encourage learning by the adult student will help make these courses a model for other security courses. The curriculum and virtual lab redesign should benefit the students so they learn the subjects and have fun with the topics, not just what it takes to pass an industry exam. Steps will need to be taken to ensure the enhancements keep moving forward. Regis will need to invest money into the program to grow it regionally and nationally. Additional courses will need to be developed so the Computer Networking student will be able grow in multiple Information Assurance disciplines.

References

Bogolea, B. and Wijekumar, K. (2004). *Information security curriculum creation: a case study*. In Proceedings of the 1st Annual Conference on Information Security Curriculum Development (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM, New York, NY, 59-65. DOI= http://doi.acm.org/10.1145/1059524.1059537.

Bowne, S. (2009). samclass.info: *Sam Bowne class information*. [Web]. Retrieved from http://samsclass.info.

Buckminster Fuller Institute. (2010). *Design science*. Retrieved from http://www.bfi.org/design-science

Cluley, G. (2010, February 18). *Please rob me site exposes danger of sharing too much information online*. Retrieved from http://www.sophos.com/blogs/gc/g/2010/02/18/pleaserobme-site-exposes-danger-sharing-information-online/.

Colorado State University. (2010, April 13). *CSU department of computer science*. Retrieved from http://www.cs.colostate.edu/cstop/index.html

Bowne, S. (2007). *Teaching hacking at college*. [Web]. Retrieved from http://media.defcon.org/dc-15/video/Defcon15-Sam_Bowne-Teaching_Hacking_at_College.m4v.

Dupuis, C, & Lambert, N. (2010). *CISSP cissp training certified information systems security professional*. Retrieved from http://www.cccure.org.

Faulkner, W. (1991). *Light in august*. New York, NY: Vintage International/Random House.

Ghafarian, A. (2007). *Ideas for projects in undergraduate information assurance and security courses*. In Proceedings of the 12th Annual SIGCSE Conference on innovation and

Technology in Computer Science Education (Dundee, Scotland, June 25 - 27, 2007). ITiCSE '07. ACM, New York, NY, 322-322. DOI= http://doi.acm.org/10.1145/1268784.1268889.

Gregory, P. (2009). *CISSP guide to security essentials*. Boston, MA: Course Technology.

Grimes, J. (2008, May 15). *Information assurance workforce improvement program*. Retrieved from www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.

Harris, S. (2007). Shon Harris CISSP video seminar [computer software]. San Antonio, TX: Career Academy.

Harris, S. (2008). CISSP all-in-one exam guide, fourth edition. New York, NY: McGraw-Hill Osborne.

Harris, S. (2010). CISSP all-in-one exam guide, fifth edition. New York, NY: McGraw-Hill Osborne.

Huffington Post. (2010, February 10). *Toyota recall 2010: more than 2 million cars recalled due to gas pedals issue*. Retrieved from http://www.huffingtonpost.com/2010/01/21/toyota-recall-2010-more-t_n_432125.html.

(ISC)2. (2009). *CISSP education & certification*. [Web] Retrieved from http://www.isc2.org/cissp/default.aspx.

Jones, A. (2003). *Adult learning: the often overlooked aspect of technical training*. In Proceedings of the 31st Annual ACM SIGUCCS Conference on User Services (San Antonio, TX, USA, September 21 - 24, 2003). SIGUCCS '03. ACM, New York, NY, 4-6. DOI= http://doi.acm.org/10.1145/947469.947471

Kolvenbach, P. (2005, September). *Jesuit education and ignatian pedagogy*. Retrieved from http://www.ajcunet.edu/Jesuit-Education-and-Ignatian-Pedagogy.

LeBlanc, C. and Stiller, E. (2004). *Teaching computer security at a small college*. In Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education (Norfolk, Virginia, USA, March 03 - 07, 2004). SIGCSE '04. ACM, New York, NY, 407-411. DOI= http://doi.acm.org/10.1145/971300.971439.

Miles, D. (2009, June 29). *Gates establishes new cyber subcommand*. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=54890

Mills, E. (2010, March 9). *Malware found on htc android phone from vodafone*. Retrieved from http://news.cnet.com/8301-27080_3-10466230-245.html.

National Security Agency. (2009). *National centers of academic excellence*. [Web] Retrieved from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

OWASP. (2009, September 29). *OWASP live cd project*. Retrieved from http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project.

Petitcolas, F. (2009, June 20). *La cryptographie militaire*. Retrieved from http://www.petitcolas.net/fabien/kerckhoffs/.

Regis University. (2010). *Computer networking degree requirements*. [Web] Retrieved from http://www.regis.edu/regis.asp?sctn=cpcis&p1=ap&p2=cn&p3=mm.

SearchSecurity.com. (2008, September 15). *CISSP essentials security school*. [Web]. Retrieved from http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1330306_mem1, 00.html.

Slatta, R. (2007, June 21). *Bloom's taxonomy*. Retrieved from http://faculty.chass.ncsu.edu/slatta/hi216/learning/bloom.htm.

Stajano, F. (2002). *Security for ubiquitous computing*. Chichester, West Sussex, England: John Wiley & Sons, Ltd.

Tiger Team. (2007). *24 karat caper*. [Web]. Retrieved from http://video.google.com/googleplayer.swf?docid=5642547759793319840&hl=en&fs=true.

Tiger Team. (2007). *The car dealership take down*. [Web]. Retrieved from http://video.google.com/googleplayer.swf?docid=-4765500972832974202&hl=en&fs=true.

Tikekar, R. and Bacon, T. (2003). *The challenges of designing lab exercises for a curriculum in computer security*. J. Comput. Small Coll. 18, 5 (May. 2003), 175-183.

Tipton, H., & Henry, K.. (2006). *Official (ISC)2 guide to the CISSP CBK*. Boca Raton, FL: Auerbach Publications.

Tzu, S., & Griffith, S. (2005). *The illustrated art of war*. New York, NY: Oxford University Press.

U.S. News, (2009). *Regis university*. [Web] Retrieved from http://www.usnewsuniversitydirectory.com/Colleges-Universities/regis/info.aspx.

WGBH Educational Foundation. (2003). *Frontline: cyber war!*. [Web]. Retrieved from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/view/

Appendix A: Regis Computer Networking Course Mapping

The current mapping for the revised Computer Networking courses is listed below in Figure A.1. The learning topics are related to each other on a week-by-week basis. The color coding was created to allow for quick reference between high level knowledge topics and ensure all topics covered in upper division courses were introduced during a lower level course.

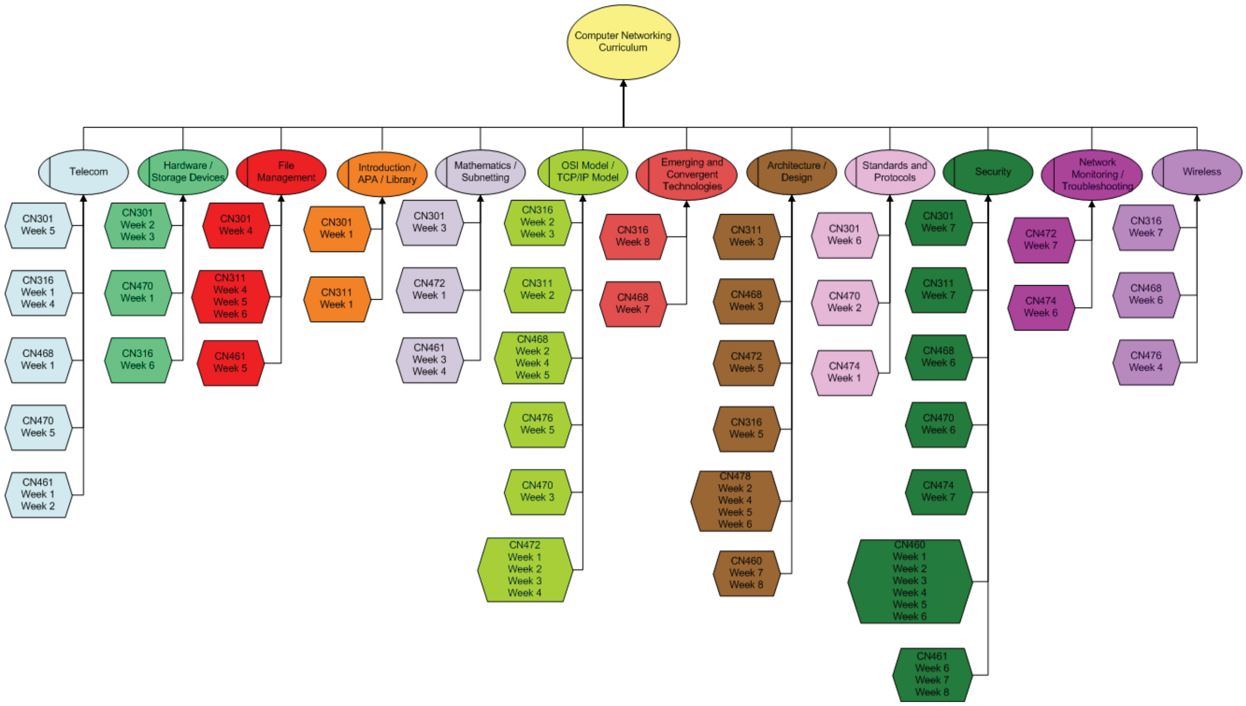

Figure A.1

Appendix B: CN460 – Fundamentals of eSecurity

CN460 was primarily authored by Professor Kim Herfurt with the assistance of Rob Winter.

Course Overview

This accelerated course CN 460, along with CN 461, will provide a comprehensive overview of the 10 security domains of the Certified Information Systems Security Professional (CISSP) exam. If students are to be successful in this course, it will be necessary to thoroughly read and comprehend all the reading assignments.

In CN 460 we will cover physical security, risk management, ubiquitous security, authentication, confidentiality, integrity, and availability. In Learning Topics 7 and 8 you will be asked to write a security plan for WigIT Corporation. Each weekly assignment that you write up to that point will guide you in writing the security plan. You will also create a presentation using PowerPoint or similar software. **You will then present to a group of your peers**. In lieu of a presentation to your peers, you may opt to create a 15-minute video presentation, including PowerPoint, and post the video to the discussion forum to be graded by other members of the course.

As you complete both CN460 and CN461, these two courses will provide an understanding of the domains in which you may choose to pursue further in-depth study.

The 10 domains of the CISSP exam are:

1. Access Control
2. Business Continuity and Disaster Recovery Planning
3. Cryptography
4. Information Security and Risk Management
5. Legal Regulations
6. Compliance and Investigations
7. Operations Security
8. Physical Security
9. Security Architecture and Design
10. Telecommunications and Network Security

The structure of each Learning Topic includes:

- Background/Rationale
- Learner Outcomes
- Readings
- Labs
- Learning Activities
- Assessments

Your facilitator will prescribe how you are to submit your assignments. For example, you may be directed to submit your assignments to the Drop Box within the course or by email to your facilitator.

Learning Topic 1: Physical Security

Background/Rationale

You should begin to have a basic understanding of the history and fundamental principles underlying information assurance. Information assurance is a fascinating study that becomes increasingly important as technology becomes more pervasive. There are many subject areas related to network security, which in the past were beyond the purview of the network engineer. However, today's network engineer must continually update his or her knowledge in order to maintain a viable network. The study of Information Assurance and cyber attacks is a lifelong learning process as attackers become ever more sophisticated. While conversation about security may initially center on hackers and crackers, there are many more facets to this study. You will learn the "behind the scenes" work conducted to strengthen our national technology infrastructure or to fortify a corporate autonomous system.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- The evolution of computing and how it relates to security
- The different areas that fall under the security umbrella
- Information warfare
- Security exploits
- A layered approach to security
- The effect of politics on security
- Security management
- The difference between administrative, technical, and physical controls
- The three main security principles

Prerequisites to be able to continue in this course – see First Class Session Assignment below.

- Regis University Ethics Statement
- Security Entrance Examination – this is a 30-minute timed exam that you may take one time only.

Readings

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.*

Ch. 2-Security Trends
Ch. 3-Information Security and Risk Management (pp. 45-76)

- APA template
- APA citation methods
- APA online citation methods

Lab/Assignment – Activity 5

Learning Activities

Note: *Activities 1, 2, and 3* ***must be completed the first day*** *of the online course.*

Activity 1: Discussion - First Class Session

1. Read Ch. 1 “Reasons to Become a CISSP”- Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.*

2. Read about the Jesuit core values on the Regis University website. See Undergraduate Core Educational Experience.

   After reading about the Jesuit core values, reflect on the Jesuit meaning of “How ought we live?” Then, complete the following statement with your reflective thoughts about ethics and Jesuit core values.

   - **Statement:** I believe ethics are formed in the following ways.

   Post your reflection as a Reply in the Discussion Forum titled “First Class Session.”

3. Read and acknowledge the Regis University Ethics Statement in the “First Class Session” Discussion Forum.
   a. ***IMPORTANT - Copy the statement at the bottom of the Ethics Statement document and paste it as a Reply inserting your name in the appropriate blanks and the date****.*

4. **Security Entrance Examination** – you must complete this exam with an 80% or higher score. The exam is self-scored. **Contact your facilitator immediately if you score lower than 80%.**
   - You will find this exam at the end of the content on the Content page. Select the Content tab. You may need to scroll down.

Activity 2: Discussion – Introductions

Introduce yourself in the Discussion Forum titled “Introductions,” and explain your reasons for becoming involved in network information assurance. Be prepared to discuss those reasons with your colleagues. Also be ready to discuss your previous experiences in computer networking, including the courses you have taken, and how these experiences may have been influenced by your experiences. Please let us know approximately how many courses you have remaining at Regis.

Activity 3: Download Course Required Resources

Download the following course materials/files the first day of this online class. Alternative text is also available in the course for the three videos.

Writing Tools
• Essential Writing Knowledge
• APA Template
• APA citation methods • APA online citation methods
Videos: download not required; however, **be sure to test your access**

to the following:
• CyberWar! (six segments)
• Tiger Team-24k heist
• Tiger Team-Exotic car heist • Cyber Protect – video game
Downloads
• Second Life browser http://www.secondlife.com

Should any of these files not be successfully downloaded, **contact your facilitator immediately** so alternative methods can be arranged.

Activity 4: Physical Security Orientation
Context: This exercise will take you to the Regis Network Operation Center (NOC) in Second Life. You will be responsible for identifying physical security deficiencies within the NOC and writing a paper describing the violations you encountered. The Regis NOC is not a private site and you may encounter non-Regis avatars.

1. Install Second Life Browser on your computer (found at http://secondlife.com)
2. Create an account and an avatar at secondlife.com. This should take you about 30 minutes.
3. You will need to pick a first name for your avatar. If you use a common name like Jim or John, your last name will be unusual, as many Jims and Johns have already registered their names.
4. You will need to also pick a unique avatar so that you may distinguish yourself from other students.
5. Tour through the help tutorial and learn how to use the avatar movement controls and the buttons at the bottom of the page.

Activity 5: Second Life Lab
Context: Please make certain you have toured through the help tutorial and learned how to use the avatar movement controls and the buttons at the bottom of the page. If you have difficulty with navigation in Second Life, you may refer to the following manuals located online in the Regis Library in the Books 24x7 section. Books 24x7 is free to Regis University faculty, staff, and students.

Books 24x7 link:
https://dml.regis.edu/login?qurl=http%3a%2f%2flibrary.books24x7.com%2flibrary.asp%3f%5eB

You may want to bookmark these two resources available to you in Books 24x7.

1. Mahar, S. and Mahar, J. (2009). *Second Life: The Official Guide.* ISBN 9780814412701. AMACOM Publishing.
2. Robbins, S. and Bell, M. (2008) *Second Life for Dummies.* ISBN 9780470180259 John Wiley and Sons.

To go to Second Life website, open Internet Explorer and put this URL into the browser or select this link: http://slurl.com/secondlife/Science%20School%20III/83/116/32

Once you have installed the browser for Second Life and created an avatar, this URL will put you on the Second Life map. You can now teleport to the Regis Physical Security Lab. Click on the "teleport now" tab. You should relocate your avatar to the Letter A on the street in front of you. If you turn your avatar, you will see a legend indicating HVAC, water lines, electrical lines, etc. These are some the items you will look for on your journey.

Second Life Lab

1. Your assignment is to tour the Network Operations Center (NOC) and discover as many Physical Security flaws as you can observe. Include recommendations for improvement of the Physical Security in the NOC. Make certain you indicate the unique moniker (nickname) assigned to your avatar. Place your avatar's name under your name on the title page of your paper.
2. Write a short paper, no more than three pages (not including title page or references), and submit your paper to the facilitator as directed. This paper must be written using APA guidelines.
3. APA information is available in your syllabus and in Learning Topic 1. You may have already downloaded the APA template and citation methods the first day of class.

Assessment
Second Life Physical Security Paper - CN Course Rubric. Submit your paper to your facilitator as directed.

Activity 6: Discussion – Second Life
Context: This activity will be a walk through the Regis Second Life Virtual Network Operations Center (NOC). You will observe Physical Security Violations and create a report of your observations.

In the Discussion Forum for this activity titled Second Life, respond to the following questions. **Read your colleagues' responses and reply to two or more of your colleagues.** For more information on strategies for responding to your colleagues, see Discussions Threading and Rubric. Your facilitator may choose from these questions or may provide other questions for your discussion.

A. Questions for Reflection and Discussion Forum:
    1. What was your experience with Second Life?
    2. What broad implications does technology like Second Life hold for learning in general?
    3. To what extent did your avatar feel unreal or even false?
    4. To what extent did you construct your avatar to be like you? To what extent did you construct your avatar to be different than you?
    5. What, if anything, concerns or alarms you about working in Second Life?
B. Read your colleagues' responses and reply to two or more of your colleagues.

Learning Topic 2: Risk Management and Ubiquity

Background/Rationale

You should have an understanding of why risk management is an important component of information assurance and how ubiquitous devices affect risk management. The media exaggerates foreign exploits of our networks, or crackers being caught and prosecuted, but these have little bearing on the daily tasks of the network engineer. Management of a secure technology infrastructure considers risk and its effects on the profitability of the organization. This may pertain to large multinational corporations or top-secret government resources that may not include financial gain. Most often, however, it involves small-to-medium-sized businesses that stretch their resources. These smaller businesses must consider the cost (or value) of what they are protecting against the potential loss of that resource. In addition to these considerations, engineers must also factor in the expanding availability of our wide area networking infrastructure. Many devices that have allowed us access to our networks are now becoming smaller, faster, and much more pervasive in our environments. We must be prepared for the “Age of Ubiquitous Computing.” The knowledge of how we should handle the security of this new age in computing is an underlying theme in this course.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- Risk management and risk analysis
- Security policies
- Information classification
- Security awareness training
- Ubiquity in computing

Readings

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.*
Ch. 3- Information Security and Risk Management (pp. 76-138)

Stajano, F. (2002). *Security for Ubiquitous Computing.*
Ch. 1-Introduction

Lab: View CyberWar! Video

Watch the video at http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/view/

Or, read the transcript of the video, which includes video chapters 1-6 scripts: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html

While viewing the video or reading the transcript, make notes of important security-related Learning Topics covered, and be prepared to discuss these with your colleagues in the Discussion Forum.

Activity 1: Discussion – CyberWar!

Context: This activity will help you understand the need for information assurance and the ongoing battle to secure our vital information infrastructure in the U.S.

Complete the lab first by watching the CyberWar! Video. Now, in the Discussion Forum for this activity, comment on your observations from the video.

Your participation in the Discussion Forum should consist of at least two substantive postings and at least two additional comments on the postings of other students. Do not simply agree with other students' opinions; use critical thinking to stimulate additional discussions from your comments. See the Discussion_Threading_and_Rubric for more details.

Activity 2: Discussion – Information Assurance
Context: Collaboration is the key to life learning and successful information assurance. You will begin the collaborative process using the Discussion Forum. There are **two threads** for this discussion activity on Information Assurance.

Start or Reply to a thread titled Part A. One of your colleagues may have already started the discussion thread for Part A.

Part A: Questions for Reflection and Discussion:
Your facilitator may choose from these questions or may provide other questions for your discussion.

1. Why do you believe (or not) that information assurance should be a critical component of network management? How would you approach this subject with your superiors at work?
2. How will what you learned about security from CyberWar! affect your perceptions of information assurance, and how will you integrate those perceptions into your future?
3. Assume WigIT Corporation is a company involved in national defense. Would that make a difference in how you would protect network assets? If so, what extra precautions might you recommend for a secure environment?
4. Read your colleagues' responses and Reply to two or more of your colleagues.

Part B: The processes of information assurance assume that there is a need to protect and guard information from dissemination, destruction, and alteration. Your facilitator may choose from these questions or may provide other questions for your discussion.

Discuss the following in a **new thread** titled Part B.

1. Excluding highly sensitive national security information, to what degree is information assurance truly warranted for the majority of the information that is gathered and stored? Is information assurance simply overreaction to unrealistic, overly dramatized threats and fears?
2. What ethical consideration does the CyberWar! video pose to the Information Assurance professional? What important ethical principles resonate with you after watching CyberWar?
3. Read your colleagues' responses and Reply to two or more of your colleagues.

Assessments
See the Discussion_Threading_and_Rubric for more details.

Learning Topic 3: Mitigating Physical Security Risks

Background/Rationale

This learning topic will inform you of the necessary steps to mitigate physical security risks and to coordinate effectively with physical security personnel to assure a secure environment for technology systems. Physical Security is often overlooked by most network engineers. It is often managed by a separate department or private security firm. If, however, the network engineer has not considered the physical aspects of security, this oversight may provide the attacker a considerable advantage. Should an exploit occur using a simple USB drive to capture secrets, or should the actual heist of network file servers be successful, it would provide the adversary with a significant advantage. Additionally, if the physical environment is not equipped with the proper safeguards to protect against power failures, fires, or acts of nature, the result could be disastrous.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- Administrative, technical, and physical controls
- Facility location, construction, and management
- Physical security risks, threats, and countermeasures
- Electrical power issues and countermeasures
- Fire prevention, detection, and suppression
- Intrusion detection systems

Readings

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.*
Ch. 6- Physical and Environmental Security

Lab: Tiger Team videos

As you view the two videos, make notes of important security-related topics and be prepared to discuss these with others in the class. Create a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to categorize your notes. If you have questions about SWOT analysis, you may find information by doing an Internet search using keywords such as SWOT analysis.

- TruTV. (Photographer). (2007). Tiger team24k heist. (21:51 minutes) [Web]. Retrieved from http://video.google.com/googleplayer.swf?docid=5642547759793319840&hl=enAssignment

- TruTV. (Photographer). (2007). Tiger team- exotic car dealer. (21:40 minutes) [Web]. Retrieved from http://video.google.com/googleplayer.swf?docid=-4765500972832974202&hl=en

Activity 1: Discussion – Tiger Team videos-SWOT Analysis

Context: These Tiger Team videos will help you understand that no matter how well an organization has protected its assets, security is an ongoing endeavor. When an individual or organization believes that their defenses are impenetrable, it poses a challenge for attackers. No matter how well you think you are defended, the attacker will usually find your vulnerabilities and exploit them.

After watching the Tiger Team videos, comment on your observations of physical security in relation to networks, and explain your observations using the SWOT analysis you created from the Lab assignment. Discuss your observations along with your colleagues' observations.

Your participation in the Discussion Forum should consist of at least two substantive postings and at least two additional comments on the postings of other students. Do not simply agree with other students' opinions; use critical thinking to stimulate additional discussions with your comments.

Activity 2: Discussion – Physical Security
Context: Share your insights and discuss your observations on physical security and your own ethical boundaries. Use the Discussion Forum titled for this activity. Your facilitator may choose from these questions or may provide other questions for your discussion.

Discuss the following questions with your colleagues.

Questions for Reflection and Discussion:

1. What security vulnerabilities did you observe that were not anticipated by those who were trying to protect themselves?
2. Could these organizations have better protected themselves? If so, what measures would you recommend to improve the physical security?
3. How should a network engineer coordinate with physical security personnel to insure the integrity of the network?
4. What physical security measures would you recommend if you were a network engineer at WigIT Corporation?
5. Given that the majority of the current hacks occur from employees on the inside, and given the current corporate ethical environment, how effective can physical security be if employees do not respect ethical boundaries? Why do you think our behavior as a society encourages this behavior?
6. What would be the best approach to take to ensure that employees entering an organization understand the implications of an insecure network and their responsibilities for helping keep the network secure? Give some examples of inadvertent security breaches in which employees may disclose information that could be used against a company.
7. Read your colleagues' responses and Reply to two or more of your colleagues.

Assessments
See the Discussion_Threading_and_Rubric for more details.

Learning Topic 4: History of Ubiquitous Computing

Background/Rationale

In this learning topic you will explore the history of ubiquitous computing and contrast its history with the reality of today. Does ubiquitous computing have a place in networks? Ubiquitous computing, while a fashionable topic for research, is becoming an ever-increasing vulnerability to our national infrastructure and autonomous systems. These pervasive devices in many instances make computing invisible. Consider for a moment General Motors (GM) Corporation's satellite network OnStar. Network help desk personnel are able to unlock vehicles for owners who have lost their keys. Remote staff are able to diagnose problems with any OnStar-equipped vehicles. We rarely think about the computational effects of fuel management or safety systems. What would happen if GM's satellite system were compromised and all GM OnStar-equipped vehicles were attacked by a virus? There are many facets to ubiquitous computing beyond the automobile.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- The history and origins of ubiquitous computing
- The evolution of ubiquitous computing to current standards
- Radio frequency identification technology
- Use of ubiquitous technology
- Security issues in ubiquitous technologies

Readings

Stajano, F. (2002). *Security for Ubiquitous Computing.*
Ch. 2-Ubiquitous Computing

Activity 1: Physical Security Plan - Midterm Paper

Context: Our networks are becoming more vulnerable because of wireless and mobile computing. Ubiquitous devices can and do pose a significant vulnerability. In this activity, you are to think outside the box and determine how to best defend against these threats.

Scenario - You are an Information Security engineer for a midsized company. The company would like to offer direct sales of its "WigIT" to its consumers on the World Wide Web. Your manager has asked you to prepare an informational paper for the Chief Executive Officer (CEO) on risk management.

1. What risks do you envision and how will you mitigate them?
2. Take into account the value of the asset(s) and data as well as the threats and vulnerabilities.
3. Prioritize these risks from greatest threat to least threat and include this analysis as an appendix to your paper.
4. Diagram your network and include that diagram as an appendix to your paper.

Write a 4-5-page paper using APA style. The title page and references do not count toward the page total.

Please refer to Grossaint's *Essential Writing Knowledge* (2001), pp. 39-44. Additionally, pay particular attention to the diagrams on pp. 47 and 48, "The Paragraph" and "Basic Five Paragraph Essay," for information about how to correctly write a college-level paper.

Assessment
CN 460 Course Rubric - Physical Security Plan. Submit your paper to your facilitator as directed.

Activity 2: Discussion - Risk Management
Context: In this activity you will have the opportunity to see your colleagues' perspectives on physical security. Think about the things that they did not think about when they wrote their papers, and discuss.

Use the Discussion Forum titled for this activity. Your facilitator may choose from these questions or may provide other questions for your discussion.

Discuss the following questions with your colleagues.

Questions for Reflection and Discussion Forum:

1. What do you believe is the single greatest risk associated with Physical Security? Defend your belief with specific examples that you have researched in the course of writing your paper this week.
2. What role does ethics play in risk management?
3. How do your conclusions about ethics affect Physical Security or Information Assurance in general?
4. Read your colleagues' responses and reply to two or more of your colleagues.

Learning Topic 5: Access Control

Background/Rationale

You will learn the fundamentals of access control to protect your infrastructure in this learning topic. Access control may be the single most important aspect of a layered network security environment. It can certainly be considered a cornerstone in the foundation of network security. Access control helps protect resources from unauthorized disclosure, modification, or destruction. The controls that a network engineer will use to protect against unauthorized access can be physical, technical, or administrative.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- Identification methods and technologies
- Authentication methods, models, and technologies
- Discretionary, mandatory, and nondiscretionary models
- Accountability, monitoring, and auditing practices
- Emanation security and technologies
- Intrusion detection systems
- Possible threats to access control practices

Readings

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.*
Ch. 4- Access Control
Stajano, F. (2002). *Security for Ubiquitous Computing.*
Ch. 3-Computer Security

Lab: Cyber Protect Game
Play the Cyber Protect game and keep track of your scores. You will need to go through the tutorial provided within the game. Keep notes on the attacks you defended against and whether you were successful or not. Use the SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to categorize your notes. Append your notes as an Appendix to your paper for Activity 1.

Activity 1: Access Control Paper
Context: Access control is perhaps the first encounter users and perpetrators will have on a network. You will discover how critically important access control is, and you will learn ways you can improve the access control methods of your users on a network. Based on the readings and your experience with the Cyber Protect game, write a 1-2-page paper using the scenario below. Be sure to use APA style. Remember, the title page and references do not count toward the page total.

Scenario - You have just been hired as the Access Control lead for your company. The company consists of the following departments: executive team, accounting, human resources, information technology, sales, and operations. You have discovered everyone in the company has full rights across the network, including domain administrator access. You need to document your findings, create an argument in favor of controlling access, and present remediation steps to the Chief Information Officer (CIO) as soon as possible. You may use the Access Control method of your choice. Please justify your position through additional research.

Please refer to Grossaint's *Essential Writing Knowledge* (2001), pp. 39-44, and pay particular attention to pp. 47 and 48, "The Paragraph" and "Basic Five Paragraph Essay," for information about how to correctly write a college-level paper.

Assessment

Access Control Paper - CN 460 Course Rubric

Activity 2: Discussion – Cyber Protect Game
Context: The Cyber Protect video game will allow you the opportunity to put to use some of the concepts you have learned and share your outcomes with your colleagues. What did I do right? What vulnerabilities did I overlook? How could I have protected my network better? These are some of the issues you should be considering in this learning activity.

The Discussion Forum should consist of at least two substantive postings and additional comments on the postings of other students. You should not simply agree with other students' opinions; use critical thinking to stimulate other discussions with your comments. Your facilitator may choose from these questions or may provide other questions for your discussion.

Begin the discussion by commenting on your observations while playing the Cyber Protect video game.

Questions for Reflection and Discussion Forum:

1. What steps (purchases) did you initially take to protect your network? Why were they successful (or not)? What would you do differently next time? Learning from a failure may be just a valuable as learning from a success, if the student recognizes the failure and makes a correction.
2. How will what you learned from Cyber Protect affect your perceptions of information assurance, and how will you integrate that perception into your future attempts at network security?
3. In the Discussion Forum, list in order of importance (first being most important) all the items you purchased that you felt best protected your network. Explain next to each item why you purchased it and why you ranked it the way you did.
4. What part do you feel Ubiquitous Computing will play in the future of enterprise computing? In 1980, Bill Gates's vision was "A computer on every desk." We now have computers on many desks. How do we define a computer today, and how does this vision fit with ubiquitous computing?

5. Read your colleagues’ responses and reply to two or more of your colleagues’ posts. Remember to respond critically but with support for your position.

Learning Topic 6: Authentication, Confidentiality, Availability, and Integrity

Background/Rationale

In this learning topic you will explore four topics and underscore the importance of each for information assurance. Authentication, while providing user accountability, may be one of the single most important factors in a secure environment. Authentication provides the user and the network with a method of non-repudiation, which in most cases clearly establishes the identity of each user. In the absence of absolute identity of your interlocutor, secure communication, encryption, and/or confidentiality are compromised. However, with strong authentication and non-repudiation, encryption and confidentiality are no longer a problem. The three basic tenets of any security endeavor are confidentiality, integrity, and availability. In the absence of any one of these three, a network has been compromised.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- Secure Transient Association
- The Resurrecting Duckling security policy model
- The many ways of being a master
- Cryptographic primitives for peanut processors
- Principles of personal privacy
- Principles of message integrity
- Principles of device integrity
- Threats to the communication channel
- Threats from mobile code
- The Cocaine Auction protocol
- Anonymity layer

Readings

Stajano, F. (2002). *Security for Ubiquitous Computing.*
Ch. 4-Authentication
Ch. 5-Confidentiality
Ch. 6-Availibility
Ch. 7-Integrity

Activity 1: Discussion - Fundamental Security Issues Paper
Context: Some of the most important concepts of data security are confidentiality, integrity, and availability. These are the fundamental concepts in data security. You will have the opportunity to explore these topics and write about your discoveries in a paper.

Using the Physical Security Plan paper that you wrote for your midterm assignment, along with the feedback on that paper from your facilitator, explain how you might integrate multifactor authentication and implement the principles of confidentiality, availability, and integrity into the WigIT website and ubiquitous devices.

Write a 2-3-page paper using APA style. The title page and references do not count toward the page total.

Please refer to Grossaint's *Essential Writing Knowledge* (2001), pp. 39-44, and pay particular attention to pp. 47 and 48, "The Paragraph" and "Basic Five Paragraph Essay," for information about how to correctly write a college-level paper.

Post your paper on the forum for your colleagues to read, **and submit your paper to your facilitator.**

Activity 2: Discussion – Reflection on Papers
Using your paper from Activity 1, discuss your findings and critically analyze the papers of your colleagues. Comment on your observations and those of your peers in the Discussion Forum. Do not just agree with the findings of others, but use "critical thinking" to develop a more powerful defense against security breaches.

Assessment
Fundamental Security Issues Paper - CN 460 Course Rubric

Learning Topic 7: Developing Your Own Data Security Plan

Background/Rationale

This learning topic will expose you to hardware, operating systems, security systems and protection systems necessary to provide a secure environment. An enterprise network consists of many devices and many levels of security. Security vulnerability in any one device or any level of the enterprise may compromise the entire system. It is incumbent upon the network engineer to understand the nature of these devices and some corresponding countermeasures to better provide for the security of the network.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- Computer hardware architectures
- Operating system architectures
- Trusted computing base and security mechanisms
- Protection mechanisms within an operating system

Readings

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.*
Ch. 5-Security Architecture and Design (pp. 281-332)

Activity 1: Data Security Paper
Context: Learning Topics 7 and 8 will allow you to integrate all that you have learned into a cohesive paper that identifies critical elements of a data security plan. This paper, through concise communication, should outline specific steps necessary for WigIT to develop a comprehensive security plan.

Scenario - Your dream job has come your way. Because of the Access Control paper you wrote for the Chief Executive Officer (CEO), and because of your knowledge of network security and ubiquitous devices, you have been promoted to the Chief Information Security Architect of WigIT Corporation.

Design the data security plan for your company, focusing on risk management, physical security, access control, application security, and ubiquitous devices, while keeping the confidentiality, integrity, and availability of the company in mind. Use the security model of your choice from the Harris text; **begin to write your paper**. Using outside resources to substantiate your assumptions will result in a higher grade.

Step 1: Write a paper

Using your knowledge from the previous six Learning Topics, **write a five-page paper** on the network you have just designed. Justify all the assumptions of the choices you have made by referencing scholarly research. Assume you have unlimited funds, but include an itemized budget in your appendix using Excel (or similar software). Because of WigIT Corporation having

Department of Defense (DoD) contracts, you will need to protect the network for national security reasons.

Please refer to Grossaint's *Essential Writing Knowledge* (2001), pp. 39-44, and pay particular attention to pp. 47 and 48, "The Paragraph" and "Basic Five Paragraph Essay," for information about how to correctly write a college-level paper.

Step 2: Create a presentation

In addition to the paper in Step 1, you will be creating a presentation ranging between 10 and15 minutes in length to present to the management team. Your **paper and presentation** will be due in Learning Topic 8. For more information, see Learning Topic 8.

Activity 2: Discussion – Information Assurance
Context: Collaboration is one of the most useful tools in a security architect's tool bag. This activity will allow you to collaborate with your colleagues and begin a lifelong connection to others involved in information assurance.

Use the Discussion Forum for this activity. Your facilitator may choose from these questions or may provide other questions for your discussion.

Discuss the following questions with your colleagues.

Questions for Reflection and Discussion Forum:

1. In your opinion, what devices are most important to a network for information assurance? Why?
2. How will you use these devices to protect your networks in the future?
3. What other things must you consider beside the physical devices and the environment to protect your network?
4. Read your colleagues' responses and reply to two or more of your colleagues.

Learning Topic 8: Data Security Plan Presentation

Background/Rationale

The security policy and the security model are two fundamental concepts in information security that you must understand. The *security policy* outlines the expectations that the hardware and software must meet to be considered in compliance. A *security model* outlines the necessary requirements to support and implement a certain security policy.

The assignment for Learning Topics 7 and 8 will be to prepare a security plan based upon a security model of your choosing.

Learner Outcomes

At the end of this Learning Topic, you will be able to understand the following concepts:

- Various security models
- Assurance evaluation criteria and ratings
- Certification and accreditation processes
- Attack types

Readings

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.*
Ch.5-Security Architecture and Design (pp. 332-388)

Activity 1: Discussion – Data Security Plan Presentation
Context: Your colleagues and your facilitator will evaluate all presentations based upon the following general guidelines and using the Evaluation of Oral Presentation form:

- Content (student displays proper use of Introduction, Body, and Conclusion in presentation)
- Presentation (Crutches, Body Control, Voice, Dynamics, Structure, Visual Aids)

Presentation Options
Option A: Stakeholders - Present your Data Security Plan to an interested body of stakeholders. The presentation of your Data Security Plan should be **at least 10 minutes but no longer than 15 minutes,** using multimedia.

Ask your stakeholders to provide you feedback during your presentation using the *Evaluation of Oral Presentation* form. You may want your stakeholders to complete this form electronically or by hard copy/paper. If the evaluation forms are returned to you in hard copy/paper, you will need to scan the returned forms. **Attach all completed forms along with your presentation.**

Option B: Video Presentation - Instead of presenting to stakeholders, create a 15-minute video presentation and post it to the Discussion Forum for this activity.

Your colleagues will complete the *Evaluation of Oral Presentation* form to *evaluate* you on your presentation. Discuss the presentations and feedback.

The presentation must be submitted to the facilitator by the specified date.

Activity 2: Data Security Plan Paper-200 points
Context: This paper is an extension of the papers you have already written in this course and will include a discussion of the Learning Topics covered during this course. You are to draft a **concise** Security Plan for the WigIT Corporation using the previous assignments that you have completed and a security model of your choice. The Data Security Plan paper must be submitted to your facilitator by the facilitator's designated due date.

This paper should be at least three and no more than five pages in length (not counting cover page and reference page). The paper should include:

- a cover page
- table of contents (optional)
- references
- appendix
- a condensed copy of the slides from your oral presentation to the stakeholders or recorded video presentation

The Data Security Plan paper must be submitted to the facilitator by the specified date.

Assessments

- **Evaluation of Oral Presentation**
- **Data Security Plan Paper -** CN 460 Course Rubric – 200 points
  Note: The same CN 460 Course Rubric will be used to assess this Data Security Plan paper.

Appendix C: CN461 – Security Breaches

CN461 was primarily authored by Rob Winter with the assistance of Professor Kim Herfurt.

Course Overview

This accelerated course, in addition to CN 460, will provide a comprehensive overview of the ten security domains of the CISSP exam. If students are to be successful in this class it will be necessary to thoroughly read and comprehend all the reading assignments.

In CN 461, we will cover telecommunications and network security, cryptography, application security, operational security, business continuity and disaster recovery, and law and investigations. In topics seven and eight you will be asked to write a business continuity / disaster recovery plan for WigIT Corporation. Each weekly assignment that you write up to that point will guide you in writing the networking and cryptography mid-term and the business continuity planning / disaster recovery final assignment. You will also create a presentation using PowerPoint or similar software. **You will then present to a group of your peers**. In lieu of a presentation to your peers, you may opt to create a 15-minute video presentation, including PowerPoint, and post the video to the discussion forum to be graded by other members of the course.

As you complete both CN 460 and CN 461, you will gain an understanding of the domains in which you may choose to pursue further in-depth study.

The 10 domains of the CISSP exam are:

11. Access Control
12. Business Continuity and Disaster Recovery Planning
13. Cryptography
14. Information Security and Risk Management
15. Legal Regulations
16. Compliance and Investigations
17. Operations Security
18. Physical Security
19. Security Architecture and Design
20. Telecommunications and Network Security

The structure of each Learning Topic includes:

- Background/Rationale
- Learner Outcomes
- Readings
- Labs
- Learning Activities
- Assessments

You will submit your assignments to the Drop Box within the course.

Learning Topic 1: Telecommunications and Network Security

Background/Rationale

With the proliferation of data across today's networks, the Information Security Professional needs to understand how these devices, networks, and protocols function and interoperate. The students will be exposed to conceptual designs and physical technologies. By studying and analyzing both the voice and data networks, students will be better able to secure a network environment and protect data.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- Open Systems Interconnection (OSI) Reference Model
- TCP/IP and many other protocols
- LAN, WAN, MAN, Internet, Extranet technologies
- Cable types and data transmission types
- Networking devices

Readings

Harris, S. (2010). *All –in- one CISSP Exam Guide Fifth Edition.*

- Read Chapter 7 "Telecommunications and Network Security", –up to Networking Services and Protocols

Learning Activities

Activity 1: Discussion – Telecommunications and Network Security, cont'd

Context: When entering an Information Assurance course, topics will be discussed between your classmates and you that may be sensitive in nature. When you post your introduction, make sure you read, acknowledge, and sign Regis University Ethics Statement.

Assignment: Use the Discussion Forum titled for this activity to post your introduction to the rest of the class and your facilitator plus read, acknowledge, and sign the Regis University Ethics Statement. Include whether you were able to successfully download the labs.

Activity 2: Telecommunications and Network Security

Context: Through the plan writing, the facilitator will be able to analyze your strengths and weaknesses in APA format, content, and understanding of the topic. Critical thinking should be used to eliminate superfluous words and present real-world examples.

Assignment: ***Working Draft*** of a Business Continuity Planning / Disaster Recovery Document - 50 points. This preliminary analysis should be working draft (very short) of your final Written Project/Oral Presentation which will be due in week 8. This will require research outside of your textbook as the topic will not be covered in-depth until later in the course. The written analysis should not exceed one double-spaced page but should include all the topics you intend to cover in your paper. Students should be prepared to present the working draft of their case during the second week of class in the forum. The topic will be a Business Continuity Planning / Disaster Recovery document for the fictitious

WigIT Corporation. A summary about this corporation was reviewed in CN460 and found for the final project for CN461.

- Use the APA template and citation methods which are attachments to this course curriculum. No citations will be necessary for an Abstract.
- Please refer to Grossaint, K. *Essential Writing Knowledge.* (2001). Denver, Colorado. Regis University p. 47 “The Paragraph” for information about how to correctly write a college level paragraph.

Assessment

CN 461 Course Rubric. Submit your paper to your facilitator as directed.

Learning Topic 2: Telecommunications and Network Security, cont'd

Background/Rationale

As an extension of Learning Topic 1, the prospective Information Security Professional will continue the journey examining the data flow on the network. You will examine local and remote access methods as well as convergent technologies. Reviewing computer networking concepts you learned in previous courses, the topics are extrapolated into not just understanding how the networks work but how to secure them. This learning topic will cover how networks expand over distance and how to secure the data transmissions. As wireless technology becomes more ubiquitous in our lives, understanding the risks and benefits from the information security perspective is critical to data security.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- Network Services
- Communications security management
- Telecommunications devices
- Remote access methods and technologies
- Wireless technologies

Readings

Harris, S. (2010). *All –in- one CISSP Exam Guide Fifth Edition.*

- Chapter 7-Telecommunications and Network Security–, continuing from Networking Services and Protocols to the end of the chapter.

Learning Activities

Activity 1: Telecommunications and Network Security, cont'd

Context: Networks are the vehicle for data. Without data, networks are not needed so the importance to securing the networks data runs on is critical. As part of a security program, you should be regularly scanning your network for new devices and determining what potential vulnerabilities may exist on your network. For this lab, you will research network and vulnerability scanners, try out a few, scan your network, identify the vulnerabilities, and suggest steps for remediation. By understanding the vulnerabilities and threats to your network, you can determine your risk level and create a more secure network.
Assignment: Vulnerability Scanning Lab

Activity 2: Discussion – Telecommunications and Network Security, cont'd

Context: You will share your insights after participating in the lab with peers on the forum and discuss observations of telecommunications and network security and their own ethical boundaries.
Assignment: Use the Discussion Forum titled for this activity. Discuss the following questions with your colleagues.
Questions for Reflection and Discussion:

1. How does Network Security impact Data Security?

2. Wireless technology is becoming more and more prevalent. What are some security risks and what are some compensating controls?
3. Identify at least two insecure protocols and methods to keep data protected.
4. As you used your vulnerability scanner on your network, did you begin to consider the ethical implications of your actions? If so, what were those considerations and what ethical values did you identify?
5. Would you do things differently on your network in the future because of these ethical considerations?
6. At which point did ethics come into play while you were testing?

Assessments

Vulnerability Scanning Lab
Discussion Forum

Learning Topic 3: Cryptography

Background/Rationale

Throughout history people have hidden data from the prying eyes of other individuals, governments, and enemies. Whether during the times of Julius Caesar, Thomas Jefferson, or today's modern world, cryptography has influenced mankind. By employing encryption and cryptographic algorithms with the storing and communications of sensitive data, the ever critical confidentiality and integrity can be achieved. By utilizing the science of cryptanalysis, an engineer can learn to decipher the puzzle and find the hidden message. The students will be exposed to cryptography on a high level and learn of its many uses.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- History of cryptography
- Cryptography components and their relationships
- Government involvement in cryptography
- Symmetric key algorithms

Readings

Harris, S. *All –in- one CISSP Exam Guide Fifth Edition. (2010).*

- Chapter 8-Cryptography, through Types of Symmetric Systems.

Learning Activities

Activity 1: Cryptography Lab

Context: Cryptography can be a challenging subject for most students to grasp due to its mathematical nature. By using the CryptoTool, you can graphically see the value of securing data without the need for looking under the algorithmic "hood."

Assignment: CryptoTool

Activity 2: Discussion – Cryptography

Context: You will share your insights after participating in the lab with peers on the forum and discuss observations of how encryption can secure our data. Be sure to critically review why encryption should or should not be used and defend your statement with academically authoritative sources.

Assignment: The forum discussion should consist of at least two substantive postings and at least two additional comments on the postings of other students. Students will not simply agree with other student's opinions but should use critical thinking to stimulate additional discussions with their comments.

Use the Discussion Forum titled for this activity. Discuss the following questions with your colleagues.

1. Why is it important to use publicly known algorithms instead of proprietary algorithms that are unknown?
2. Review some common websites to find areas that should use HTTPS instead of HTTP. Document why they should be encrypted and not transmitted in plain text.

3. Define your values as they relate to cryptography. Is the use of cryptography always ethical?
4. When would the use of cryptography not be ethical?

Assessment
Crypto Tool Lab
Discussion Forum Rubric

Advanced Preparation
Students should begin the reading for Week 4 in anticipation of writing their mid-term paper.

Learning Topic 4: Cryptography, cont'd

Background/Rationale

During the second set of two learning topics on cryptography, you will expand your knowledge on the different algorithms and uses. Continuing on the cryptographic trek, you have the opportunity to examine more complex concepts. Building off of the CrypTool lab, you will learn and understand how cryptographic attacks occur and why only time-tested algorithms should be used to protect sensitive data. Understanding how attacks can occur will prepare the engineer on how to better defend their data.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- Asymmetric key algorithms
- Public key infrastructure (PKI) concepts and mechanisms
- Hashing algorithms and uses
- Types of attacks on cryptosystems

Readings

Harris, S. (2010). *All –in- one CISSP Exam Guide Fifth Edition.*
Chapter 8-Cryptography, from Types of Asymmetric Systems to the end of the chapter.

Learning Activities

Activity 1: Mid-Term Paper-Networking and Cryptography

Context: As the perimeter of our networks expand to a point where the egress point is nearly indistinguishable, threats that may impact our environment contain a more devastating risk. Securing the data proactively becomes the critical task regardless of whether it is in motion or at rest. In this activity, the student is to think outside the box and determine how to best defend against this ever moving perimeter.

Scenario: You have been assigned the task of securing the data on WigIT Corporation's network using encryption. By evaluating how to protect the network across all seven layers of the Open Systems Interconnection (OSI) Reference Model, define ways to safeguard the corporate data. Utilizing your knowledge from the Telecommunication and Network Security as well as Cryptography lessons since the beginning of the course, develop your Cryptography strategy for the network paper.

Paper: Write a five page paper using APA style. The title and reference pages do not count toward the page total. The research paper should include academic resources outside of the required reading.

- Please refer to Grossaint, K. *Essential Writing Knowledge*. (2001). Denver, Colorado. Regis University pp. 39-44 and pay particular attention to pp. 47 and 48 "The Paragraph" and "Basic Five Paragraph Essay" for information about how to correctly write a college level paper.

Assessment

CN 461 Course Rubric - Mid-Term Paper-Networking and Cryptography – 100 points. Submit your paper to your facilitator as directed.

Learning Topic 5: Application Security

Background/Rationale

Application security should be applied as a built-in technology and not a bolt-on remediation step. The lack of application security is demonstrated by the massive amount of security breaches due to the lack of security controls within websites and client applications. Engaging the project development teams during the inception and design phases can help the Information Security engineer make sure security is woven into the fabrics of information technology systems. By the students examining how application vulnerabilities occur, ways to test the software for errors, and mitigate the risks, the potential Information Security professional will be able to reduce their exposure to their environment. Application security is often overlooked by more-seasoned network security professionals but current threats are exploiting the applications more now than ever.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- Various types of software controls and implementation
- Database concepts and security issues
- Data warehousing and data mining
- Software life-cycle development processes
- Change control concepts
- Object-oriented programming components
- Expert systems and artificial intelligence

Readings

Harris, S. (2010). *All –in- one CISSP Exam Guide, Fifth Edition.*

- Chapter 11-Application Security

Learning Activities

Activity 1: Application Security Lab

Context: Using the LabRat / WebGoat lab on the live CD, you will be able to learn and understand how application-based attacks can occur in your networks. By analyzing the attack methods, you will be able to determine if your own networks are vulnerable to application attacks and develop mitigation strategies.

Assignment: LabRat / WebGoat – Follow the lab instructions for Learning Topic 5 using WebGoat. Use the SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis to categorize your notes. Your facilitator will specify how to submit your notes from this lab.

Activity 2: Thesis Statement

Context: You should continue the working draft created in the first learning topic by providing a solid thesis statement for the final project.

Assignment: The student is expected to create the thesis statement for their final assignment. The student should view the thesis statement document as provided in Week 1.

Activity 3: Discussion – Application Security

Context: After completing the lab, share your insights with your peers on the forum and discuss observations of application security and their own ethical boundaries.

Use the Discussion Forum titled for this activity. Discuss the following questions with your colleagues.

1. When should application security be applied to a project? If it is not applied during this phase, what is the best way to make sure it is added?
2. Over the years Microsoft has moved from one of the worst offenders of securing their applications to one of the more respected software vendors. Why have other software vendors not moved to a more secure model?
3. Is a software vendor's lack of adequate security a violation of ethics? Is it a fiscal decision? Do vendors have a responsibility to their shareholders?
4. A completely secure environment is an unusable environment for the users. How can security work in an atmosphere that mandates usability over safeguards?

Assessments

LabRat / WebGoat Lab – 25
Discussion Forum Rubric – 25 points

Advanced Preparation

Students should begin researching and outlining in anticipation of writing their final project paper and presentation.

Learning Topic 6: Operations Security

Background/Rationale

Day in and day out information technology departments are tasked with making their systems work to the upmost service levels while reducing costs. Operations Security assists the technology department by controlling access, reviewing logs, monitoring activity, and performing audits. The maintenance of the systems ensures the unauthorized disclosure, alteration, and destruction of data is minimized. You will learn how operational security functions within information technology. Configuration management and administrative responsibilities are paramount to setting up an information system's environment for success. Daily activities will either open the organization up to additional risk or reduce the threats. Whether reviewing redundant systems, communications security, or current threats, you will understand what it takes to manage a day-to-day information security operation.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- Administrative management responsibilities
- Operations department responsibilities
- Configuration management
- Trusted recovery states
- Redundancy and fault-tolerant systems
- E-mail security
- Threats to operations security

Readings

Harris, S. (2010). *All –in- one CISSP Exam Guide Fifth Edition.*

- Chapter 12-Operations Security

Learning Activities

Activity 1: Operations Security

Context: An old English proverb states "Time and tide waits for no man". Those who procrastinate on the final project will have difficulties completing the tasks successfully.
Assignment: The deliverable for the week is a strong thesis statement. Your facilitator will respond to your thesis statement within 72 hours of receipt but you should continue to work on your research during this time period. You should continue working on the final assignment throughout this week.

Activity 2: Discussion – Operations Security

Context: Operations security is one of the only domains where most security professionals will spend at least part of their career. You should spend time contemplating and critical thinking about the risks to your environment. The Discussion Forum Questions will help to facilitate this process.
Assignment: Use the Discussion Forum titled for this activity. Discuss the following questions with your colleagues.

1. Security patches can help reduce the attack platform a malicious software package can use to compromise systems. Should vendor supplied patches be applied to systems as soon as they are released? Why or why not and provide rationale?
2. Certain protocols such as SMTP transmit information in plain text. Students should choose an insecure protocol, (do not chose a protocol already chosen by another student) and research a secure alternative. Inform the other students about your research and how to implement the protocol securely. Students should post a brief explanation of the protocol while researching it in depth.
3. With all of the web-based threats, what do you believe is the most secure web browser today and why?

Assessments
Discussion Forum Rubric– 25 points

Advanced Preparation
Students should be concluding their research and outlines in anticipation of writing their final project paper and presentation.

Learning Topic 7: Business Continuity Planning and Disaster Recovery

Background/Rationale

After September 11, 2001, several companies who were established in the World Trade Center buildings never opened their doors again. Some of the corporations in the New Orleans area during Katrina did not adequately prepare for such a disastrous storm. Events can occur outside of our control. Organizations need to be prepared for a disaster whether by a terrorist or mother nature. Preparations, however, do not stop once the Disaster Recovery and Business Continuity plans have been created. These plans should be continually tested and retested to validate strategies. Hardware and software are continually updated and these plans must keep up with infrastructure changes within an organization. By taking steps to prepare for events outside the control of the company, the security engineer can help make sure the business thrives in the face of catastrophes.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- Project initiation steps
- Recovery and continuity planning requirements
- Business impact analysis
- Selecting, developing, and implementing disaster and continuity plans
- Backup and offsite facilities
- Types of drills and tests

Readings

Harris, S. (2010). *All –in- one CISSP Exam Guide Fifth Edition.*

- Chapter 9-Business Continuity and Disaster Recovery

Learning Activities

Activity 1: Business Continuity Planning / Disaster Recovery Plan Paper – 200 points

Context: Learning topics seven and eight will allow you to integrate all you have learned into a cohesive paper that identifies critical elements of a business continuity / disaster recovery plan. This paper, through concise communication, should outline specific steps necessary for WigIT Corporation to develop a comprehensive disaster recovery plan.

Scenario: WigIT Corporation maintains financial and personally identifiable information on its servers for the United States Department of Defense (DoD). Such data is required by law or regulation to be kept in a secure manner. The student is expected to design a disaster recovery solution that allows the company to adhere to the strict government standards while remaining viable during a catastrophe. This solution should take into account that the corporation must continue operations with their electronic storefront, the security of corporate data, and provide the business with the capacity to experience minimal disruption.

Assignment: Using your knowledge from the previous six learning topics, write a concise five page paper on the BCP/DR plan for WigIT Corporation. The paper length does not include the title and reference pages. Points will be deducted for too many or too few pages. Be sure to use APA style and formatting. Provide a rationale for your assumptions underlying the recommendations you have made by referencing scholarly research. For an assignment of this length, five to ten academically referenced sources are considered acceptable. One of these references may be your textbox. Assume you have potentially unlimited funds, but include an itemized budget as an appendix (not considered part of the five pages) using Excel (or similar software). Because of WigIT Corporation having DoD contracts, you will need to adhere to strict controls for protecting the network against national security concerns such as internal and external terrorist threats, natural disasters, and foreign governments.

- Please refer to Grossaint, K. *Essential Writing Knowledge*. (2001). Denver, Colorado. Regis University pp. 39-44 and pay particular attention to pp. 47 and 48 “The Paragraph” and “Basic Five Paragraph Essay” for information about how to correctly write a college level paper.
- This paper should be at least three and no more than five pages in length (not counting cover page and reference page). The paper should include:
    - a cover page
    - table of contents (optional)
    - references
    - appendix
    - a condensed copy of the slides from your oral presentation (Activity 2) to the stakeholders or recorded video presentation

Activity 2: BCP/DR Presentation

Context: Regis promotes the motto of “Learners becoming Leaders”, but what is a leader? A leader has the ability to stand out from the crowd and lead by example. As part of this, the leader needs to be able to verbalize their stance to others. In keeping with this theme, this course will require you to present your BCP/DR to others in the course.

Scenario: The scenario is the same as you wrote for your final paper. While the WigIT Corporation management team is the specified audience, you may specify which executive department members will be receiving the presentation.

Assignment: Create a presentation ranging between 10-15 minutes in length to present to the management team of WigIt Corporation. Include a condensed copy of the slides along with your BC/DRP plan/paper.

- Submit to the facilitator, as directed.

Activity 3: Timely Evaluation of Fellow Students’ Presentations

Context: Assessing the presentations from other students will help you expand your knowledge by looking at the problem through a different set of eyes.

Assignment: Review at least two (2) other presentations and provide constructive feedback back to your fellow classmates. Responses of “Good job!” and “I agree” will be considered inadequate. If a presentation already has two responses, select a different presentation to review.

Assessments

BC/DRP paper - 200

BD/DRP presentation – 100

Peer Presentation Evaluation - 25

Learning Topic 8: Laws and Investigations

Background/Rationale

Thieves steal, con artists scam, vandals deface, and criminals commit crimes. Thirty years ago these events would have occurred in the physical world but today they can also be found in the virtual world. Knowing what motivates these attackers and the appropriate recourse supplies the security professional with the tools to identify, investigate, and pursue justice. When fighting cyber crime an investigator is only as good as his reputation. A highly developed sense of ethics is critical to a lasting long term reputation. Straddling the moral code of conduct is not an option if one intends to remain in the Information Assurance industry.

Learner Outcomes

At the end of this topic, you will be able to understand the following concepts:

- Computer crimes and computer laws
- Motives and profiles of attackers
- Various types of evidence
- Laws, directives, and regulation
- put into effect to fight computer crime
- Computer crime investigation process and evidence collection
- Incident-handling procedures
- Ethics pertaining to information security professionals and best practices

Readings

Harris, S. (2010). *All –in- one CISSP Exam Guide Fifth Edition.*

- Chapter 10-Legal, Regulations, Compliance, and Investigations

Activity:

Complete any tasks not yet finished. This includes the final paper, presentation, and student peer presentation evaluation.

Appendix D: Course Labs

The labs were primarily authored by Rob Winter with the assistance of Professor Kim Herfurt.

Vulnerability Scanning

Activity: CN461 - Learning Topic 2

Context: In this lab, you research network and vulnerability scanners, try out a few, scan your network, identify the vulnerabilities, and suggest steps for remediation.

Learning Outcome: You will understand how to identify assets on their networks, review those assets to determine risk levels, and document remediation steps.

Task:

1. This lab will have you scanning networks. Please make sure if you do not own the network you will be scanning, you obtain permission first. Administering a network is not the same as owning it. If you do not have a network to scan, scanning your local computer is acceptable. If you do have VMWare or similar virtualization software, you may run this lab against the live CDs included in this course.
2. Research at least three different network and vulnerability scanners such as, but not limited to, NMap, Nessus, and Retina. Sectools.org has a wonderful list of well-known network and vulnerability tools. Be sure to stay with tools that are considered reputable to ensure minimal infection of malware during this lab (e.g. Anti-Virus 2009 is NOT a good tool and is considered malware).
3. Scan your network and document your results.
4. Review the results and determine what vulnerabilities are acceptable on your network. As an example, port 80 is usually acceptable for a web server however Windows file sharing (ports 135-139 TCP and UDP, and port 445 TCP and UDP) available directly from the Internet is usually discouraged.
5. Document what remediation steps you would take to better secure your network. Be sure to justify you remediation steps (or lack of remediation steps).
   <u>Potential scenarios</u>
   a. If you do have a intranet web server running on port 80 but do not want it accessible from the Internet, you may want to deny inbound port 80 to that server on your firewall.
   b. If you only want the Regis Academic Research Network (ARNe) to be able to access the server, you may want to permit 65.102.82.136-65.102.82.143 inbound on port 80 and deny the rest.
   c. If your computer shows a vulnerability for Adobe Acrobat Reader, what would you do to fix the problem, if anything?

3.Submit your document to your facilitator through the course dropbox.

Critical Thinking Questions

a.After researching the different network and vulnerability scanners, why did you choose one over the rest?
b.After identifying potential vulnerabilities on a network, how would you decide which vulnerabilities should be fixed first, second, third, etc?
c.What compensating controls would you put around an asset you cannot remediate (e.g. the vendor of the application, appliance, or server will not support the device if it is patched)
d.How makes the ultimate decision on how much risk is acceptable for a particular solution? How did this play into the scanning and remediation of your network for this lab?

Notes on APA style - Please make sure you review appropriate APA style. If you need help with the formatting, please ask your facilitator. Don't let your paper get downgraded due to improper format. Below are a few of the sites found useful to other students regarding APA formatting:

1. Purdue OWL - http://owl.english.purdue.edu/owl/resource/560/01/
Wonderful site with lots of APA examples

2. APA Citation Online - http://citationmachine.net/index2.php
Online site that formats your references for you

3. Reference Point (purchased software) - http://www.referencepointsoftware.com/order.htm
Purchased software that formats the paper including fonts, title page, body, and references. This software is available through the Regis Bookstore or through the vendor.

4. Regis SmartThinking - http://www.regis.edu/regis.asp?sctn=cur&p1=spsug&p2=tutor
The College for Professional Studies will provide 10 hours of FREE tutoring or writing assistance for one year for all CPS students where you can access live tutors by e-mail, chat, or phone. This service is also found in every online course in the Resources tab. This service will not write the papers for you, but will provide some idea as to issues found in the papers.

CrypTool

Activity: CN461 – Learning Topic 3

Context: The student will be able to test different cryptographic algorithms against a block of text.

Learning Outcome: The student will use critical thinking and learned knowledge to explain simple differences of cryptography.

Task: Complete the steps below then answer the Critical Thinking Questions. Answers should be in APA paragraph format. Submit your answers to your facilitator using the course dropbox.

Steps:

Setup

•Download CrypTool from http://www.cryptool.org, if it has not already been downloaded.
•Run the installer and choose the defaults for the install.
•Once the tool is installed, click File and Open. Select 'CrypTool-en.txt' and click Open.

Symmetric

•Choose Crypt/Decrypt, Symmetric (classic), Caesar/ROT-13
•Change Key entry from Alphabet character to Number value. Enter the number value as 3.
•Click Encrypt.
•Repeat the process but click Decrypt instead. Note the results.
•Close all windows except the original 'CrypTool-en.txt' file.

Asymmetric

•Click Crypt/Decrypt, Asymmetric, and RSA Encryption.
•Choose the default key and click Encrypt. Note the results.
•Click Crypt/Decrypt, Asymmetric, and RSA Decryption. Enter the PIN code of '1234' and click Decrypt. Note the results.
•Close all windows except the original 'CrypTool-en.txt' file.

Hash

•Click Indiv. Procedures, Hash, and SHA-1.
•Click Store hash value to HEX format.
•Decrypt the value back to the original value. Note the results.
•Close all windows except the original 'CrypTool-en.txt' file.

Analysis

•Click Analysis, Symmetric Encryption (modern), and Rijndal (AES)

•Change the key length to 256 bit and click Start.
•Note the remaining time. Click cancel twice.
•Click Analysis, Symmetric Encryption (classic), Ciphertext-Only, and Caesar.
•Review the results while you click OK, OK, and Decrypt. Note the time it took to analyze a Caesar encrypted file.

Critical Thinking Questions

1.Why did the encrypt/decrypt cycle work with the symmetric encryption?
2.Why did the encrypt/decrypt cycle require a separate process for the asymmetric?
3.What method did you use to decrypt the hash value back to the original data?
4.If Caesar and AES are both symmetric encryption algorithms, explain the reason for the time difference during the analysis.

Notes on APA style - Please make sure you review appropriate APA style. If you need help with the formatting, please ask your facilitator. Don't let your paper get downgraded due to improper format. Below are a few of the sites found useful to other students regarding APA formatting:

- Purdue OWL - http://owl.english.purdue.edu/owl/resource/560/01/
  Wonderful site with lots of APA examples
- APA Citation Online - http://citationmachine.net/index2.php
  Online site that formats your references for you
- Reference Point (purchased software) - http://www.referencepointsoftware.com/order.htm
  Purchased software that formats the paper including fonts, title page, body, and references. This software is available through the Regis Bookstore or through the vendor.
- Regis SmartThinking - http://www.regis.edu/regis.asp?sctn=cur&p1=spsug&p2=tutor
  The College for Professional Studies will provide 10 hours of free tutoring or writing assistance for one year for all CPS students where you can access live tutors by e-mail, chat, or phone. This service is also found in every online course in the Resources tab. This service will not write the papers for you, but will provide some idea as to issues found in the papers.

WebGoat / LabRat

Activity: CN461 – Learning Topic 6

Context: Using the open source Live CD provided by the Open Web Application Security Project containing several security projects and tools the student will be able to simulate several common application vulnerabilities.

Learning Outcome: The student will be able to experience common programming issues and understand, through documentation, ways to mitigate these problems.

Task

Description

5. Download LabRat from 'http://appseclive.org/content/downloads'. The Live CD is available in ISO (a compressed disk image), VMDK (VMWare's disk image and used with VMWare Player), or VDI (Virtual Box hard drive image).
6. Once the desired method has been downloaded, initiated, and loaded, click the KDE K Menu (Comparable to the Start Button for Windows), select OWASP Live CD, and click WebGoat Manager (WebGoat Admin GUI).
7. When the WebGoat Manager opens, click 'Start'.
8. When the Status changes from 'Stopped' to 'Started on port 8080', click 'Go to WebGoat'.
9. The username is 'guest' and the password is 'guest'.
10. On the 'Thank you for using WebGoat!' screen, click 'Start WebGoat'.
11. The following labs should be completed. Note the 'Hints' link that can be used when the student is stuck. Care should be taken to document the steps taken so they can be reproduced. When the student has completed each lab, a short write-up consisting of no less than a single properly structured paragraph and no more than two pages in APA format should be completed stating how the common application vulnerabilities should be mitigated.
    a. Lab 1 - Click 'Code Quality' and select 'Discover Clues in the HTML'. Programmers often forget to remove information from their code. Complete the steps and document the username and password.
    b. Lab 2 - Under 'Authentication Flaws', click 'Forgot Password Basic Authentication'. Complete the steps and document the discovered password.
    c. Lab 3 - Choose 'Insecure Communication' and 'Insecure Login'. The student will need to make sure Wireshark from K Menu, OWASP Live CD, Wireshark (Packet Sniffer). Click 'OK' to the 'Running as root' warning. Click 'Capture' and 'Interfaces'. On the 'Capture Interfaces' window click 'Start' under the device 'lo' and IP address of 127.0.0.1 (the loopback address). Click 'Submit' on the WebGoat lab. Go back to Wireshark and click 'Capture' and 'Stop'. In Wireshark right-mouse click one of the packets using the HTTP protocol and select 'Follow TCP Stream'. Complete the steps and document the password, whether subsequent tried are shown in plain text, and the protocol used.
    d. Lab 4 - Click 'Injection Flaws' and work through the 'String SQL Injection' and 'Database Backdoors' labs. The other labs within 'Injection Flaws' can be completed but only these two are required for the assignment. Complete the steps and document the findings.

e. Lab 5 - Under ‘Denial of Service’, click ‘Denial of Service from Multiple Logins’. Use your knowledge of SQL Injection to complete this task. Complete the steps and document your information.

Delivery

- Lab is to be completed by the end of week 6.
- Complete the lab and email it to the instructor. Make sure the information and mitigation documentation steps comply with APA format.

Links

AppSecLive, . (2009). *Downloads*. Retrieved from http://appseclive.org/content/downloads

OWASP. (2009*). Category:OWASP live cd project*. Retrieved from http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project.

Assessment

Student will be graded on completeness of lab and explanation of the mitigation steps.