**University of Virginia**

**School of Continuing and Professional Studies**

**Summer 2014**

**Class Overview: General Class Information**

**Instructor Name and Contact Information**: Dr. Charles Pak, CISSP, CISM, CRISC, SSCP, MCSE, MCT, CCNA, ITIL, Security+; (443)610-7986, [cp9hb@virginia.edu](file:///\\office-pc\data\UVA\BUS5030\cp9hb@virginia.edu)

**Year and Term**: Summer 2014

**Class Title**: BUS 5030 Designing Dynamic Security Architecture

**Credit Type**: 3 Graduate Credits

**Class Description**:

Explore the building blocks needed to implement a life-cycle security system. Instruction focuses on how to analyze internal applications, computing platforms/network infrastructure, and corporate objectives with an eye toward designing flexible security architecture that is best suited for the enterprise including how to define security architecture and what security architecture describes. Case studies are used to illustrate key security architecture concepts and methods. The latest challenges and the new default expectations of enterprise security will be explained. Explain what the new default expectations are of the systems. Commonly used terms in security architecture (e.g., Policy, Access Controls, and Authentication Server) will be defined.

**Required Text**: Designing Security Architecture Solutions: ISBN-10:**0471206024**| ISBN-13:**978-0471206026** | Wiley, Edition: **1**

**Learning Outcomes**:

On successful completion, the student will be able to:

* 1. Understand common hacker strategies, attack methods, tools, and attack classes, e.g., distributed denial of service, root kits, sniffer programs and Trojan horses.
  2. Develop strategies and architecture countermeasures to protect an environment from hacker exploits and tactics. Focus is on routers, operating systems, firewalls, IDS and other network systems.
  3. Plan and coordinate the implementation of holistic security measures in multiple layers within the IT networking environment.
  4. Develop requirements and planning documentation for security risk assessment, vulnerability assessment and penetration testing.
  5. Understand how to apply the various options available for IT security architecture to a given set of requirements.
  6. Design a process to track vulnerabilities and security incidents and plan for applying vendor related patches and updates in an ongoing basis.
  7. Design and develop security architecture analysis models.
  8. Demonstrate the uses and usefulness of security architectures.
  9. Describe security design and the tools for documenting it.
  10. Describe key building blocks and the mortar for gluing them into a coherent whole.
  11. Recommend guiding principles and specific recommendations for consideration in every security architecture design.
  12. Apply cloud Security architecture
  13. Review of Resilience Management Models

**Course activities to meet objectives:**

The course will be delivered by online instruction, lecture notes and reports from group collaboration on case studies. PowerPoint presentations supplemented by the textbooks, white papers articles, and the instructor lead discussions will be provided. Interaction with classmates, especially with on-line discussions is encouraged.

**Preparation and student expectations:**

**Reading Assignments:** Students are expected to read all assigned readings before the class in which the topics will be discussed. Students are also encouraged to read as much of the suggested readings as possible to enhance their insight into the course subject matter. The instructor will provide additional materials such as related white papers, reprinted articles, and URLs to related material located on public Internet servers.

As a preliminary preparation for this course, it is necessary that the students effectively review all materials and complete the individual assignments by the due dates. Late assignments will be reflected by a reduction in grade.

**Course Delivery:**

The course will be conducted entirely online using a combination of lecture, class discussion and group case study exercises. This course will be taught via a series of modules, each of which will introduce an important topic, fundamental or building block required for successfully designing security architectures across enterprise network environments. Some of the modules will provide a high-level overview of fundamental principles that will be covered in greater detail in other courses in the Information Security Management Certificate program. Some of the modules will survey subject matter of other information technology programs, as well. Each of the modules will be supported by readings in the assigned textbook, white papers and articles.

**Assessment Components**:

Delivery Mode Expectations (Classroom/Internet and Web-based classes, specify any live (synchronous) meetings, dates, times, and location of delivery):

The course will be conducted entirely online using a combination of lecture, class discussion and group case study exercises. This course will be taught via a series of modules, each of which will introduce an important topic, fundamental or building block required for successfully designing security architectures across enterprise network environments. Some of the modules will provide a high-level overview of fundamental principles that will be covered in greater detail in other courses in the Information Security Management Certificate program. Some of the modules will survey subject matter of other information technology programs, as well. Each of the modules will be supported by readings in the assigned textbook, white papers and articles.

**Course Policy:**

* **Class attendance is mandatory.** If unforeseeable circumstances cause students to miss three or more classes, that student is expected to discuss the situation in advance with the instructor to make up assignments.
* All work done outside of class and in conjunction with the course must be typed and double-spaced. The instructor reserves the right to impose other formatting instructions as the need arises e.g., footnotes should be included at the end of assignments instead of at the bottom of each page, etc.
* Work is due when scheduled. No exceptions. Failure to meet deadlines will result in reduced grades.
* Students should be prepared to devote several hours per week to conduct research in support of weekly assignments.
* Before each class, each student should study the assignment chapters in the text and designated reading materials assigned by the instructor. Each student is expected to participate in classroom discussions and case study activity.
* **Special Needs:** If you are a student with special needs it is your responsibility to notify your instructor within the first week of class. Written documentation is required. Please go to the following Websites to review your rights and responsibilities as a student: <http://virginia.edu/vpsa/rights.html> and http://www.virginia.edu/studenthealth/lnec/.

**Technical Specifications: Computer Hardware:**

* Computer with basic audio/video output equipment
* Internet access (broadband recommended)
* Microsoft Word

**Technical Support Contacts:**

* Login/Password: [scpshelpdesk@virginia.edu](mailto:scpshelpdesk@virginia.edu)
* UVaCollab: [collab-support@virginia.edu](mailto:collab-support@virginia.edu)
* BbCollaborate (Elluminate) Support: <http://support.blackboardcollaborate.com>

**U.Va. Policies**

**SCPS Grading Policies:** Courses carrying a School of Continuing and Professional Studies subject area use the following grading system:  A+, A, A-; B+, B, B-; C+, C, C-; D+, D, D-; F.  S (satisfactory) and U (unsatisfactory) are used for some course offerings. For noncredit courses, the grade notation is N (no credit). Students who audit courses receive the designation AU (audit). The symbol W is used when a student officially drops a course before its completion or if the student withdraws from an academic program of the University. Please visit [SCPS Grades](http://www.scps.virginia.edu/audience/students/grades)

**University Email Policies:** Students are expected to check their official U.Va. email addresses on a frequent and consistent basis to remain informed of University communications, as certain communications may be time sensitive. Students who fail to check their email on a regular basis are responsible for any resulting consequences.

**University of Virginia Honor System:** All work should be pledged in the spirit of the Honor System at the University of Virginia.The instructor will indicate which assignments and activities are to be done individually and which permit collaboration. The following pledge should be written out at the end of all quizzes, examinations, individual assignments and papers: “I pledge that I have neither given nor received help a on this examination (quiz, assignment, etc.)”. The pledge must be signed by the student. For more information please visit [Honor System](http://records.ureg.virginia.edu/content.php?catoid=28&navoid=747)

**Special Needs:** It is the policy of the University of Virginia to accommodate students with disabilities in accordance with federal and state laws. Any SCPS student with a disability who needs accommodation (e.g., in arrangements for seating, extended time for examinations, or note-taking, etc.),should contact the Student Disability Access Center (SDAC) and provide them with appropriate medical or psychological documentation of his/her condition. Once accommodations are approved, it is the student’s responsibility to follow up with the instructor about logistics and implementation of accommodations. Accommodations for test taking should be arranged at least 14 business days in advance of the date of the test(s). Students with disabilities are encouraged to contact the SDAC*:* 434-243-5180/Voice, 434-465-6579/Video Phone, 434-243-5188/Fax. Further policies and statements available[: U.Va. Department of Student Health](http://www.virginia.edu/studenthealth/sdac.html#types)

For further policies and statements about student rights and responsibilities, please see [U.Va Website](http://www.scps.virginia.edu/audience/students) (<http://www.scps.virginia.edu/audience/students>)

**The Academic Honor System**

***The University of Virginia academic honor system*** embodies many of Mr. Jefferson's principles. The purpose of the Honor System is to sustain and protect a community of trust in which students can enjoy the freedom to develop their intellectual and personal potential. The concept of an honor system implies that students commit themselves to the pursuit of truth. At the Division of Continuing Education, course is conducted in the spirit of the Honor System. The instructor will indicate which assignments and activities are to be done individually or which permit collaboration. The following pledge should be written out at the end of all quizzes, examinations, individual assignments and papers: "I pledge that I have neither given nor received help on this examination (quiz, assignment, etc.)" The pledge should be signed by the student. If you have any questions about the Honor System, you may contact the Honor Committee in Charlottesville, VA at 804-924-3452.

**Competencies**

**Knowledge, skills and abilities in the following areas will be obtained upon completion of this course:**

* Foundation for effective IT security management
* Open access computing environments
* Life cycle and holistic security concepts
* Define and describe the function of firewalls
* Define and describe virtual private networks
* Define and describe intrusion detection systems
* Define and describe authentication systems
* Review of other point solutions such as SSH and SSL
* The basis for privacy, authentication and data integrity in open networks
* The role of encryption, digital signatures and authentication
* The concept of untrusted networks
* The potential threat of the Internet
* Fundamental knowledge of hacker attack classes
* Basic understanding of port scanning
* Hacker tools and strategies
* How hackers operate in networks
* Multi layer security approach
* Hardening and streamlining network infrastructure to achieve life-cycle security gains.
* Define and describe the process of hardening of network systems
* Host versus network based IDS systems
* Design security assessment programs
* Host versus network based vulnerability assessments

**Evaluation and Grading Criteria:**

Student grades will be determined by class participation, course assignments, examinations, case study work, and other projects. Students are expected to complete all assigned reading and problems and take all examinations by the assigned dates.  Students will be familiar with and conduct themselves in accordance with the UVA Honor Code.    To get the most out of the class, students should read the chapters and complete assignments on time and stay current with the material.  Also, students should log on the class page frequently to keep current with questions/answers and other postings.

The mid-term examination will be given for the primary purpose of determining the progress of students with the course subject matter. The mid-term will be based upon class lectures, reading assignments and textbook content.

The final examination will cover the fundamental concepts and their application, which will be practiced in conjunction with completing the case studies. The examination will be used to ensure the concepts and principles of the course are mastered so that the student realizes a satisfactory grade. The examination will also assure the development of a workable knowledge base in information security management and the proficiency in applying the concepts to address real world requirements and situations.

The instructor will assign weekly assignments that will draw upon student’s knowledge and proficiency with security concepts and principles challenge their ability to implement practical cost-effective architecture solutions and collaborate as a team as necessary in the real world.

Each student must select and complete a term project. The instructor will approve the topic. Review sessions and interim check points will be conducted in an agreed upon time to assist students to focus on the subject matter and formulate the term paper outline.

**Suggested term paper & outline (15 – 20 pages)**:

* Table of contents with detailed sub headings (maximum of 4 levels)
* Executive summary of the topic/subject and what was accomplished
* Introduction (purpose, methodology, structure)
* Formulation of the problem and elaboration
* Management, measures and techniques relevant to the topic
* Approach methodology/presentation/body of discussion
* Conclusions and/or requirements
* References and bibliography
* Appendices

The following tables feature the percentage breakdown of each assignment area towards the final grade and the grading scale.

**Assignment Area Percentages:**

|  |  |
| --- | --- |
| **Graded Items** | **Percentage** |
| Attendance and quality of participation (incl. online) | 25% |
| Research Paper | 15% |
| Course assignments/weekly forums | 30% |
| Term project | 30% |
| **Total** | **100%** |

**Grading Scale:**

|  |  |
| --- | --- |
| A | 95-100 |
| A- | 90-94 |
| B+ | 86-89 |
| B | 82-85 |
| B- | 79-81 |
| C+ | 75-78 |
| C | 71-74 |
| C- | 68-70 |
| F | 67 and Below |

1. **Textbook/Reference Materials:**

Designing Security Architecture Solutions (Wiley Desktop Editions) [Paperback] by:Jay Ramachandran

**Schedule of Assignments**

|  |  |  |  |
| --- | --- | --- | --- |
| **Wee Week** | **Week of** | **Topic Discussion** | **Weekly Text-based Assignments** |
| 1 | May 29 | Introduction: Class overview, objectives  Why Security Architecture?  Hacker threats, attacks, case reviews Certifications, professional organizations, and further resources. |  |
| Defining Requirements  -Operational, Management, & Technical  Policy and Planning  Design Guidelines  -Access Control, Authentication, Confidentiality, Integrity, Availability |
| 2 | June 5 | Intro to cryptography concepts, Internet standards and network review to include wireless topics |  |
|  |  | Security Systems:  Intrusion Detection Systems  Firewalls  Virtual Private Networks  Authentication Servers  Access control (Biometrics) |  |
| Security System Continued |
| 3 | June 12 | Security Assessments  Penetration Testing and Audits |  |
| Control and Monitoring Systems |
| 4 | June 19 |  |  |
| PKI Components and Applications  Perimeter Architecture Models  Public Access  Remote Access  Internet POP |
| 5 | June 26 | Internal Architecture Models  Users  Administrators |  |
| Architecture review  Other Architecture Components |
| 6 | July 3 | Cloud Security Architecture |  |
| 7 | July 10 | Resiliency Security Model – application and implementation planning:   * Case study/online review and assessment |  |
| 8 | July 17 | Building Blocks  Glue  Platform hardening and application security |  |
| Case Studies  A look at industry best practices |

**Case Study Project**

**Cyber Marketing, INC. (CMI)**

Cyber Marketing, Inc. (CMI) is a marketing company that markets its products and services to thousands of its clients across the North America. As a marketing company, the products and services catalog is an important corporate asset to keep up-to-date for its clients. In order to keep its products and services updated at all times, its corporate IT infrastructure plays an important role in processing data within and between the company and the clients. The following organization chart depicts the CMI executive management team.



Figure 1 CMI Management Organizational Chart

**Background and You Role**

You are the Cybersecurity Manager educated, trained, and hired to protect the physical, logical, and operational security of CMI’s corporate information system.

CMI has experienced several cyber-attacks from outsiders over the past a few years. In 2013, the Oracle database server was attacked and its customer database lost its confidentiality, integrity, and availability for several days. Although the company restored the Oracle database server back online, its lost confidentiality damaged the company reputations. CMI ended up paying its customers a large sum of settlement for their loss of customer data confidentiality. Another security attack was carried out by a malicious virus that infected the entire network for several days. While infected, the Oracle and e-mail servers had to be shut down to quarantine these servers. In the meantime, the company lost $1.2Million in revenue and intangible customer confidence.

**CMI Enterprise Network Infrastructure**



You are responsible for a corporate WAN spanning 10 remote facilities and interconnecting those facilities to the central data processing environment. Data is transmitted from a remote site through a VPN appliance situated in the border layer of the routing topology; the remote VPN connects to the internal Oracle database to update the customer data tables. Data transaction from the remote access to the corporate internal databases is not encrypted.

A bulk of the data processing for your company is handled by Oracle database on a high end super computer. The trusted computing based (TCB) internal network is situated in a physically separated subnet. This is where all corporate data processing is completed and internal support team has its own intranet web server, a SUS server, an internal DNS, an e-mail system, and other support personnel workstations. Each corporate department is segregated physically on a different subnet and shares the corporate data in the TCB network.

**OTHER CONSIDERATIONS**

1. Recently, your network engineers report that they’ve noted a significant spike in network traffic crossing into the internal networks. They report that they cannot be certain what or who is generating this traffic, but the volume and frequency of traffic is certainly abnormal. The management is very concerned over securing the corporate confidential data and customer information.
2. Increasingly, CMI’s CEO Thompson attempts to outsource IT competency. In fact, you’ve been told of a plan from COO Willy to outsource network management and security functions away from your department and to a service integrator. COO Willy warns you that the political environment will only become more contentious over time; you must make a compelling case as to what value your department can bring over an integrator that can provide secure services at 40% less annual cost than you.
3. The interrelationship between data and operations concerns you. Increasingly, some of the 10 remote sites have been reporting significant problems with network latency, slow performance, and application time-outs against the Oracle database. The company’s business model is driving higher and higher demand for data, but your capability to respond to these problems are drastically limited.
4. Mobility is important for the organization to interact with the customers and other co-workers in near real-time. However, the CEO is concerned with the mobility security and would like to research for the best practice for mobility computing. The CEO is willing to implement a BYOD policy if security can be addressed.
5. Employees enjoy the flexibility of getting access to the corporate network using a WiFi network. However, the CEO is concerned over the security ramifications over the wireless network that is widely open to the company and nearby residents.
6. The company plans to offer its products and services online and requested its IT department to design a Cloud Computing based e-commerce platform. However, the CEO is particularly concerned over the cloud computing security in case the customer database was breached.

**ASSIGNMENTS**

* + Identify and describe the organizational assets and their values.
  + Conduct a risk assessment, and impact analysis of the CMI corporate network.
  + Make a list of access points internal and external (remote).
  + Design a secure authentication technology and network security for CMI.
  + Make assumptions for any unknown facts.
  + List all known vulnerabilities you can identify in this environment and address them by proposing a new design. You may use any combination of technologies to harden authentication process and network security measures.
  + Address the CEO’s concern over the mobility security and design a secure mobile computing (smart phones, tablets, laptops, etc.) in terms of authentication technologies, privacy and data protection.
  + Describe the BYOD policies, standards, procedures, and guidelines to accommodate both the user demand of BYOD and the productivity at work without compromising security.
  + Identify wireless vulnerabilities and recommend what safeguards, authentication technologies, and network security to protect data & privacy should be implemented.
  + Design a cloud computing environment for the company with a secure means of data protection at rest, in motion and in process.
  + Based on the CMI corporate network description, write a disaster recovery plan for CMI.

**Case Study Paper Grading Rubric**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | | | | | |
|  | **Poor** | **Fair** | **Good** | **Excellent** | **Percent** |
| **Organization** | Sequence of information is difficult to follow. (**0 – 7**) | Reader has difficulty following work because student jumps around. (**8 – 14**) | Student presents information in logical sequence which reader can follow. (**15 – 22**) | Information in logical, interesting sequence which reader can follow. (**23 – 30**) | 30% |
| **Content Knowledge** | Student does not have grasp of information; student cannot answer questions about subject. (**0 – 12**) | Student is uncomfortable with content and is able to demonstrate basic concepts. (**13 – 24**) | Student is at ease with content, but fails to elaborate. (**25 – 37**) | Student demonstrates full knowledge (more than required). (**38 – 50**) | 50% |
| **Grammar and Spelling** | Work has significant spelling errors and/or grammatical errors. (**0 – 2**) | Presentation has several and/or grammatical errors. (**3 – 4**) | Presentation has a couple misspellings and/or grammatical errors. (**5 – 7**) | Presentation has no misspellings or grammatical errors. (**8 – 10**) | 10% |
| **APA Formatting** | Work has significant formatting errors (i.e. references page, title page, spacing, citations). (**0 – 2**) | Work has several formatting errors (i.e. references page, title page, spacing, citations). (**3 - 4** ) | Work has a few formatting errors (i.e. references page, title page, spacing, citations). (**5 – 7**) | Work has no formatting errors (i.e. references page, title page, spacing, citations). (**8 - 10** ) | 10% |