IS314T
Security Architecture of Common IT Platforms
[Onsite]

Course Description:

This course is an introduction to security architecture of common IT platforms and applications. Course topics include how to identify security needs within the network, in operating systems, databases and applications and over the Web. The course also includes instruction on how to implement different security measures.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IS311T Internetworking Infrastructure and Operations or equivalent

Credit hours: 4

Contact hours: 60 (36 Theory Hours, 24 Lab Hours)

SYLLABUS: Security Architecture of Common IT Platforms

Instructor: _____

Office hours: _____

Class hours: _____

MAJOR INSTRUCTIONAL AREAS

1. Identify the threats at different layers of the OSI and TCP models.
2. Identify network controls and countermeasures.
3. Implement a Virtual Local Area Network (VLAN).
4. Implement Dynamic Host Configuration Protocol (DHCP).
5. Identify routing and switching technologies.
6. Implement ACLs on routers.
7. Identify vulnerabilities of switches and routers.
8. Discuss defense-in-depth and how network segmentation and low-level design can accomplish it.
9. Describe wireless networking technologies such as switches, access points and repeaters.
10. Describe point-to-point and omni-directional wireless technologies.
11. Identify the different wireless standards.
12. Identify the different wireless security standards.

COURSE OBJECTIVES

After successful completion of this course, the student will have the opportunity to:

1. Discuss the process of designing secured network architecture.
2. Explain how to implement communication and network security.
3. Create user and group accounts, and explain the role of assigning rights, policies, and permissions in an operating system.
4. Explain how to secure an operating system.
5. Implement data integrity in a database.
6. Implement Web security options.
7. Illustrate the process of securing Application layer.
8. Implement business function applications integrity through proper validation of security controls such as patches.

Related SCANS Objectives

1. Evaluate the set of procedures, tools, or computers and their programs that will create secure network architecture for an organization.
2. Troubleshoot the problems in the security architecture of an organization.
3. Demonstrate how components of a network interact within and outside the network, applying technical skills.
4. Create secure network architecture for an organization.
5. Identify the knowledge of security requirements of the organization with the best application of information assurance practices.
6. Classify the availability, integrity and confidentiality of data in an orderly manner to

ensure the specific secure requirements of the organization.

7. Acquire security related data and evaluate it for the purpose of implementing secure network architecture for an organization.
8. Interpret security data, which effectively communicate the justification of related security information.
9. Process security configurations using computers.
10. Solve security issues as a member of an information technology team.
11. Evaluate a decision regarding security structure of the organization and other related problems through negotiation with others.

TEACHING STRATEGIES

The curriculum is designed to promote a variety of teaching strategies that support the outcomes described in the course objectives and that foster higher cognitive skills. Delivery makes use of various media and delivery tools in the classroom.

COURSE RESOURCES

Student Textbook Package

- *Security Architecture of Common IT Platforms. Pearson Custom Publishing, 2006.*
- Security+ LabSim CD
- Security+ LabSim lab manual on CD

  - The textbook is a custom publication taken from: *Network Security Architectures by Sean Convery, CCIE® No. 4232 and Security in Computing, 3rd Edition by Charles P. Pfleeger and Shari Lawrence Pfleeger.*

References and Resources

ITT Tech Virtual Library

Login to the ITT Tech Virtual Library (http://www.library.itt-tech.edu/) to access online books, journals, and other reference resources selected to support ITT Tech curricula.

- General References

  - >Reference Resources>Database Security and Auditing, Hassan A. Afyouni, Thompson Course Technology, January 2006
  - >Reference Resources>National Institute of Standards and Technology (NIST) publications
    - Special Publication 800-77: Guide to IPsec VPNs, December 2005
    - Special Publication 800-68: Guidance for securing Windows XP
    - Systems for IT Professionals, October 2005
    - Special Publication 800-34: Contingency Planning Guide for Information Technology Systems, June 2002
  - >Program Links> Information Systems Security (ISS)> Information Systems Security Association (ISSA)
  - >Program Links> Information Systems Security (ISS)> Computer Security Institute
  - >Program Links> Information Systems Security (ISS)> Recommended Links > CERT Coordination Center
  - >Program Links> Information Systems Security (ISS)> Recommended Links > Common Vulnerabilities and Exposures

  - Books

The following books related to this course are available through the ITT Tech Virtual Library

- Books > Books 24x7 > Exchange 2000 Server Administrator's Bible > Chapter 22 – Securing Your System
- Books > Books 24x7 > Microsoft SQL Server 2000 Operations Guide > Chapter 3 – Security Administration
- Books > Books 24x7 > Expert Web Services Security in the .NET Platform > Chapter 2 – Windows Security (for securing IIS 6.0)

- Periodicals

  - **Periodicals>EbscoHost**
    Ebsco databases contain numerous publications; EbscoHost is a search engine that can search all the databases simultaneously.

- Other Resources

  - http://compnetworking.about.com/library/weekly/aa010701d.htm (Introduction to VPNs) - March 6, 2006
  - http://cr.yp.to/qmail/guarantee.html (q-mail security) - March 6, 2006
  - http://cr.yp.to/mail.html (Internet mail) - March 6, 2006
  - http://cr.yp.to/smtp.html (SMTP resource) - March 6, 2006
  - http://cr.yp.to/immhf.html (Internet mail header) - March 6, 2006
  - http://www.fefe.de/arprelay/ (ARP relaying) - March 6, 2006
  - http://www.itworld.com/nl/unix_sec/11292001 (Securing UNIX)
  - http://www.f-secure.com/virus-info/tips.shtml (Network security tips) - March 6, 2006
  - http://www.microsoft.com/technet/itsolutions/howto/sechow.mspx (Microsoft security how-to guides) - March 6, 2006

- http://www.eventid.net/ (Analysis of audit logs) - March 6, 2006
- http://www.itworld.com/WhitePapers/Cisco_SAFE/ (Cisco Networks) - March 6, 2006
- http://www.networkingunlimited.com/whitepapers.html (Cisco white papers) - March 6, 2006
- http://www.enterasys.com/products/whitepapers/ (Security white papers) - March 6, 2006
- http://www.microsoft.com/windowsserver2003/techinfo/overview/security.mspx (Windows 2003 Security Services) - March 6, 2006
- http://www.microsoft.com/isaserver/evaluation/whitepapers/default.mspx (Microsoft ISA (Internet Security and Acceleration) white papers) - March 6, 2006
- http://www.microsoft.com/resources/documentation/msa/idc/all/solution/en-us/oag/oagc12.mspx (Microsoft IDC - Internet Data Center) - March 6, 2006
- http://nvd.nist.gov/ (National Vulnerability Database) - March 6, 2006
- http://csrc.nist.gov/publications/nistpubs/index.html (NIST Special Publications) - March 6, 2006
- http://www.vmware.com/products/ws/ (Virtual Machine Workstation documentation) - March 6, 2006
- http://www.gpoguy.com/ (Group Policy resource) - March 6, 2006
- http://web.mit.edu/kerberos/www/ (Kerberos) - March 6, 2006
- http://www.securitydocs.com/ (Network Security White Papers) - March 6, 2006

All links to web references outside of the ITT Tech Virtual Library are always subject to change without prior notice.

EVALUATION & GRADING

COURSE REQUIREMENTS

1. **Attendance and Participation**

   Regular attendance and participation are essential for satisfactory progress in this course.

2. **Completed Assignments**

   Each student is responsible for completing all assignments on time.

3. **Team Participation (if applicable)**

   Each student is responsible for participating in team assignments and for completing the delegated task. Each team member must honestly evaluate the contributions by all members of their respective teams.

Evaluation Criteria Table

Final grades will be based on the following weighted categories:

GRADE CATEGORY	WEIGHT
Participation	10%
Writing Assignments	10%
Research Assignments	10%
Lab Assignments	20%
Quizzes	10%
Project 1	15%
Final Project	25%
Total	**100%**

Grade Conversion Table

Final grades will be calculated from the percentages earned in class as follows:

A	90 - 100%	4.0
B+	85 - 89%	3.5
B	80 - 84%	3.0
C+	75 - 79%	2.5
C	70 - 74%	2.0
D+	65 - 69%	1.5

D	60 - 64%	1.0
F	<60%	0.0

COURSE OUTLINE

Readings:

- **Unit 1**: All the concepts will be covered in the class; therefore, the specified readings are merely for your reference.
- **For all units, except Unit 1**: It is recommended that you complete the readings before attending the class.

Unit #	Activities for the Unit
1	• **Read** ○ **Chapter 1:** Network Security Axioms, Pages 3-26. ○ **Chapter 7:** Network Security Platform Options and Best Deployment Practices, Pages 265-294. ○ **Chapter 14:** Designing Your Security System, Pages 585-614. ○ http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm (DMZ) • **In-class Discussion # 1** • **Research Assignment # 1** • **Lab #1**
2	• **Read** ○ **Chapter 6:** General Design Considerations, Pages 191-264. ○ http://www.erg.abdn.ac.uk/users/gorry/eg2069/async.html (about 4 pages) ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=3633&chunkid=0747201059 (Protocols) • **Research Assignment # 1**

3	• **Read** ○ **Chapter 4:** Network Security Technologies, Pages 119-166. ○ **Chapter 6:** General Design Considerations, Pages 191-264 (Review) ○ **Chapter 16:** Campus Security Design, Pages 669-703 ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=7324&chunkid=0859705610 (LAN switch Types) ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=7324&chunkid=0996709760 (Switching Services) • **Quiz #1** • **Writing Assignment #1** • **Lab # 1**
4	• **Read** ○ **Chapter 5 :** Device Hardening, Pages 167-190. ○ http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/08w2kada.mspx ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=9753&chunkid=0553728243 (User Management) ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=5465&chunkid=0638131609 (Creating Local and Domain User Accounts) • **In-class Discussion #1** • **Lab #1**
5	• **Read** ○ **Chapter 8:** Designing Trusted Operating Systems, Pages 295-378. ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=5465&chunkid=0690525037 (Understanding Groups) ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=5465&chunkid=0898

	064391 (Managing and Creating User Accounts) http://ittlibrary.books24x7.com/viewer.asp?bookid=5465&chunkid=0717503192 (Working With roaming User Profiles) http://ittlibrary.books24x7.com/viewer.asp?bookid=10479&chunkid=0944303417 (Logon) http://ittlibrary.books24x7.com/viewer.asp?bookid=9208&chunkid=0523181669&rowid=889 (Enforcing Privilege Management) • **Writing Assignment #1** • **Research Assignment #1** • **Labs #1 and #2** • **In-class Discussion # 1**
6	• **Read** o **Chapter 10:** Database Security, Pages 401-456. o http://ittlibrary.books24x7.com/viewer.asp?bookid=9208&chunkid=0523181669&rowid=889 • **Quiz #1**
7	• **Read** o **Chapter 3:** Secure Networking Threats, Pages 53-118. o **Chapter 11:** Identity Design Considerations, Pages 457-488. o **Chapter 10:** Database Security, Pages 401-456. (Review) o http://ittlibrary.books24x7.com/viewer.asp?bookid=9204&chunkid=402469098 (Operations Security Concepts) • **Writing Assignments #1 and #2** • **Research Assignment #1**
8	• **Read** o **Chapter 12:** IPsec VPN Design Considerations, Pages 489-548. o **Chapter 13:** Supporting-Technology Design Considerations, Pages

	549-559. • **Writing Assignment #1** • **Lab #1**
9	• **Read** ○ **Chapter 9:** Common Application Design Considerations, Pages 379-400. • **Start Project #1/Submit Project #1** • **Lab #1**
10	• **Read** ○ **Chapter 2:** Security Policy and Operations Life Cycle, Pages 27-52. ○ **Chapter 15:** Edge Security Design, Pages 615-668. ○ **Chapter 18:** Secure Network Management and Network Security Management, Pages 723-766. ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=10904&chunkid=0221255862 (Security Patching) (about 13 pages) ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=9204&chunkid=0124156876 (Business Continuity Planning) (about 13 pages) ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=9204&chunkid=0549413732 (Disaster Recovery Planning) (about 15 pages) ○ http://ittlibrary.books24x7.com/viewer.asp?bookid=9204&chunkid=0128475446 (Security Management Concepts and Principles) (about 9 pages) • **Research Assignment #1** • **Writing Assignment #1**
11	• **Read**

	○ **Chapter 20:** Conclusions, Pages 795-804. • **Course Project**

INTENT/INTERFACE

The focus of the onsite course is to build on the basic principles of securing common information technology operating systems and applications. The course will help students understand why information technology architecture security concepts are important to them as IT professionals. Each lesson will present the current real-world examples and tables that will help students to connect the importance of information assurance to the business environments around them. The strategy employed in this course will be to introduce significant examples and thought-provoking questions related to the need to secure information, maintain information assurance, and plan an effective security policy based on business needs.

