King Saud University
College of Computer and Information Sciences
Department of Computer Engineering

CEN 448 – SECURITY AND INTERNET PROTOCOLS (3-0-1)
Semester II, Academic Year 2011-2012
Required Course: Time (SMW 10:00-11:00 AM)

Course Description (catalog):
Overview, Security Concepts, Attacks, Services; Block Ciphers; Block Cipher Operation; Public-Key Cryptography and RSA; Cryptographic Hash Functions; User Authentication Protocols; Transport-Level Security; Wireless Network Security; IP Security; Intruders; Malicious Software; Firewalls.

Prerequisites: - Courses CEN 445.
- Topics
- Computer Networks

Textbook(s) and/or Other Required Materials:
Primary:
- William Stallings, *Cryptography and Network Security*, Prentice-Hall, 5/E, 2011.

Supplementary:
- Alfred Menezes, Paul van Oorschot and Scott Vanstone, "Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)", CRC Press, 1/E, 1996. Available online at: http://www.cacr.math.uwaterloo.ca/hac/.
- Lecture Notes, Selected Articles from the World Wide Web.

Course Learning Outcomes: This course requires the student to demonstrate the following:

1. Identify the main security attack types and standard security terminology.
2. Understand concepts such as block ciphers, symmetric/asymmetric encryption, digital signatures, conditional and unconditional security.
3. Recognize the ethical aspects of using computer systems.
4. Apply encryption and hash algorithms by hand and/or using calculator.
5. Assess security vulnerabilities in authentication protocols.
6. Implement network security applications and protocols.
7. Identify how to implement security at different system and network layers.
8. Decide appropriate firewall types and design firewall rules
9. Design good security policies based on needs and threats.

Major Topics covered and schedule in weeks:

Introduction, Security Concepts, Attacks, Services	1
Block Ciphers and their Operation	3
Public-Key Cryptography and Hash Functions	2
User Authentication Protocols	1
IP and Transport-Layer Security	2
Wireless Network Security	1
Intruders and Malicious Software	2
Firewalls	2
Review and Evaluation	1

Assessment Plan for the Course

Homework/Quizzes	10%
Projects	10%
Midterm 1	20%
Midterm 2	20%
Final Exam	40%

Tentative Out-of-class Assignments and dates

		Date
Homework 1	Introduction, Classical Encryption	
Homework 2	Classical Encryption, Block Ciphers and DES	
Homework 3	Advanced Encryption Standard	
Homework 4	Public-Key Encryption, RSA	
Homework 5	Digital Signature and Authentication Protocols	
Homework 6	IP and Transport Layer Security	
Project 1	Using Encryption Software	
Project 2	Using Public-Key and Digital Signature	
Project 3	Using Protocol Analyzer to Analyze SSL Protocol	
Project 4	Using Password Cracker	
Midterm 1	Covers Chapters 1, 2, 3, 5, 6, 9 (Stallings 5E)	21-03-2012
Midterm 2	Covers Chapters 11, 14, 15, 16 (Stallings 5E)	02-05-2012

- Make sure your email address registered at edugate is accurate and current.
- Announcements and course notes will be posted on the course website: http://faculty.ksu.edu.sa/mdahshan/Pages/CEN448.322.aspx.
- Homework must be submitted using Jusur LMS http://jusur.edu.sa/jusur/ no later than specified date.
- Homework assignments and projects must be done individually.
- You may not share your answers with others.
- Plagiarism is an academic misconduct and will not be tolerated.

Contribution of Course to Meeting Curriculum Disciplines:

Curriculum Discipline	Percentage
Mathematics and Basic Science	10
Engineering Science	60
Engineering Design	30
General Education	

Relationship of Course to Student Outcomes

Outcome	Student Outcome Description	Level of Contribution
(a)	an ability to apply knowledge of mathematics, science, and engineering	
(b)	an ability to design and conduct experiments, as well as to analyze and interpret data	
(c)	an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability	
(d)	an ability to function on multidisciplinary teams	
(e)	an ability to identify, formulate, and solve engineering problems	✓
(f)	an understanding of professional and ethical responsibility	
(g)	an ability to communicate effectively	
(h)	the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context	✓
(i)	a recognition of the need for, and an ability to engage in life-long learning	
(j)	a knowledge of contemporary issues	✓
(k)	an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.	

Current Instructor, Department, Office Hours and Date:

Dr. Mostafa Hassan Dahshan
Department of Computer Engineering
Bldg: 31, room: 2190
Office Hours: Sunday 12-2PM, Wednesday 10AM-2PM, and by appointments
Email: mdahshan@ksu.edu.sa
Office Phone: 46-76703
Semester II, AY 2011-2012