Network Security

MET CS 690

Instructor

Stuart Jacobs, MSc, CISSP
Lecturer, Computer Science Department Metropolitan College Boston University

Office hours: By prior arrangement.

Office Address: 808 Commonwealth Ave., Room 250. Boston, MA 02215.

E-mail: sjjacobs@bu.edu

Course Description

This course covers advanced network security issues and solutions. The course starts with consideration of why network security is necessary, network vulnerabilities and the types of attacks networks need to defend against. Discussion of basic security concepts of security services, and the role played by encryption and hash algorithms along with issues and approaches for key management follow. Particular focus and emphasis are then covered regarding to network security capabilities and mechanisms (Access Control on wired and wireless networks), IPsec, Firewalls, Deep Packet Inspection and network flow monitoring. A discussion of network application security (Email, Web, P2P, etc.) is presented followed by consideration of network utility (DNS, NTP, etc.) and management protocols (SNMP, RMON, etc.), management tools (Syslog, vulnerability scanning, penetration texting, etc.) and concluding with a review of necessary operational security processes and activities. Discussion of remote access issues, such as dial-up servers, modems, VPN gateways and clients are included.

Prerequisites

- MET TC535 or MET CS625 Data Communications and Computer Networks;
- Familiarity with OSI and TCP/IP protocol stack;
- Background familiarity with binary numbers, prime numbers, binary, hexadecimal decimal conversions, etc.; and
- Familiarity with computer programming concepts. Strong networking and software background is expected.

Required Course Book

Network Security -- Private Communication in a Public World, Charlie Kaufman, Radia Perlman and Mike Speciner, 2nd Edition, Prentice-Hall, 2002, ISBN 0-13-046019-2

Courseware

This course uses Online Campus (Blackboard). Once the course starts all students must use the Online Campus Dashboard internal messages service. Both sections are expected to use Online campus:

- for reading assignments beyond text book assigned reading,
- Submitting homework assignments,
- Submitting lab exercises,

- Taking on-line quizzes,
- Participating in discussion threads,
- Taking the on-line final examination and practice final exam, and
- All course related email correspondence.

All lectures will be recorded and archived. The archived recordings will be accessible from the Online Campus Dashboard under the heading "Live Classroom (Question & Answer) Sessions".

Class Policies

1) Attendance & Absences
   - Students enrolled in section A1 are expected to attend all scheduled on-campus lectures.
   - Students enrolled in section E1 are required to attend the four scheduled on-campus lectures (**9/11, 10/2, 11/6, 12/11** and the final exam on **12/18**) but are welcome to attend any other scheduled on-campus lectures in person or via Adobe Connect.
   - Students in either section must notify the instructor in advance if unable to attend any on-campus lecture.
   - On-campus lectures will be held in room 264 at 808 Commonwealth Ave. second floor.
2) Assignment, Lab Exercise and Discussion Completion & Late Work
   - Homework assignments are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. If a student will be unable to submit an assignment by its due date, the student must contact the Instructor or Facilitator **in advance** to avoid a grade of zero (0) on the submitted material.
   - Lab exercises: are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. If a student will be unable to submit a Lab exercise by its due date, the student must contact the Instructor or Facilitator **in advance** to avoid a grade of zero (0) on the submitted material.
   - Student postings to discussion topic after the listed closing dates will not be counted when calculating a student's discussion grades.
3) Academic Conduct Code – Cheating and plagiarism will not be tolerated in any Metropolitan College course. Such activities/behavior will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code:

   http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html.

   Such activities/behavior includes copying (even with modifications) of another student's work or letting your work to be copied. Your participation in interactions with the instructor and your classmates is encouraged, but the work you submit must be your own. Collaboration is not permitted.

Class Meetings, Lectures, Assignments, Lab Exercises & Examinations

Class Meetings

- The on-campus face-to-face class schedule for Fall 2017 MET CS 690 A1/E1 is:

9/11 (Monday)	*Class 1*
9/18 (Monday)	Class 2
9/25 (Monday)	Class 3
10/2 (Monday)	*Class 4*
10/10 (Tuesday)	*Class 5*
10/16 (Monday)	Class 6
10/23 (Monday)	Class 7
10/30 (Monday)	Class 8
11/6 (Monday)	*Class 9*
11/13 (Monday)	Class 10
11/20 (Monday)	Class 11
11/27 (Monday)	Class 12
12/4 (Monday)	Class 13
12/11(Monday)	*Class 14*
12/18 (Monday)	*Final Exam on-campus*

Dates in this color and *italic* identify sessions where the A1 and E1 sections both meet on campus

On-line Live sessions

- There will be a number of one hour on-line sessions conducted by your Instructor which will be held Thursday evenings on 9/7, 9/14, 9/21, 9/28, 10/5, 10/12, 10/19, 10/26, 11/2, 11/9, 11/16, 11/30, 12/7, and 12/14 at 8:00 PM ET

  To access these sessions, use the link "MET CS690 Live Classroom" on the "Online Classrooms/Offices" Blackboard page

  During these on-line sessions the Instructor will hold a question & answer period.. Attendance is not required at these sessions but highly recommended. All on-line sessions will be recorded and archived for student access.

CS 690 Semester Meeting Times

- On the next page is a complete calendar for the fall 2017 that depicts the dates of all CS 690 classes and dates and time of class on-line sessions. This calendar is definitive and supersedes all other sources of information.

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
9/4 Labor Day	9/5	9/6	9/7 On-line session 8pm	9/8	9/9	9/10
9/11 **Class-1 joint** ***Module 1***	9/12	9/13	9/14 On-line session 8pm	9/15	9/16	9/17
9/18 **Class-2**	9/19	9/20	9/21 On-line session 8pm	9/22	9/23	9/24
9/25 **Class-3** ***Module 2***	9/26	9/27	9/28 On-line session 8pm	9/29	9/30	10/1
10/2 **Class-4 joint**	10/3	10/4	10/5 On-line session 8pm	10/6	10/7	10/8
10/9 Columbus Day	10/10 **Class-5**	10/11	10/12 On-line session 8pm	10/13	10/14	10/15
10/16 **Class-6** ***Module 3***	10/17	10/18	10/19 On-line session 8pm	10/20	10/21	10/22
10/23 **Class-7**	10/24	10/25	10/26 On-line session 8pm	10/27	10/28	10/29
10/30 **Class-8** ***Module 4***	10/31	11/1	11/2 On-line session 8pm	11/3	11/4	11/5
11/6 **Class-9 joint**	11/7	11/8	11/9 On-line session 8pm	11/10	11/11	11/12
11/13 **Class-10** ***Module 5***	11/14	11/15	11/16 On-line session 8pm	11/17	11/18	11/19
11/20 **Class-11**	11/21	11/22	11/23	11/24	11/25	11/26
11/27 **Class-12** ***Module 6***	11/28	11/29	11/30 On-line session 8pm	12/1	12/2	12/3
12/4 **Class-13**	12/5	12/6	12/7 On-line session 8pm	12/8	12/9	12/10
12/11 **Class-14 joint**	12/12 Last class day	12/13	12/14 On-line session 8pm	12/15	12/16 Exam Start	12/17
12/18 **Final Exam**	12/19	12/20	12/21 Exam End	12/22	12/23	12/24

Assignments

- All homework assignments are identified within the Online campus Study Guide.
- File names for assignment documents should be:

  CS690-HW<number>-<student last name>.doc

  An example assignment document file name is:

  CS690-HW5-Jacobs.doc

  Student submissions which fail to follow this direction will have 5 points deducted!
- Student assignment submissions must be no more than 4 pages in length, be single spaced**,** use 12 point Times Roman type font and 1" margins on all sides. Student submissions which fail to follow this direction will have points deducted!
- Include the file name in the header and a page number in the footer of you assignment submission document. Student submissions which fail to follow this direction will have points deducted!
- Title cover pages are not required and should not be used;
- Assignment submission documents MUST be in Word 2003 or Word 2007 file formats that are NOT encoded in XML;
- Quoted material and citations must follow the American Psychological Association (APA) format with a reference section at the end of a student's submitted work. Please refer to the http://www.apastyle.org/ web site for guidance on following the APA style guide.
- Students are required to comply with the directions contained within the document **APA Criteria for Course.pdf** whenever the work of others is used as part of a student's assignment submission. Failure to do so will result in points being deducted for the assignment grade.
- Wikipedia is a useful starting point for finding information about a subject BUT NOT an acceptable direct reference source. One should only reference or quote from primary (source) documents.

Lab Exercises

- Lab exercises are identified within the Assignment description document for each course module.
- File names for lab exercise documents should be:

  CS690-LAB<number>-<student last name>.doc

  An example lab exercise document file name is:

  CS690-LAB5-Jacobs.doc

  Student submissions which fail to follow this direction will have 5 points deducted!
- Students should enter their lab exercise answers direct within each lab exercise document and then submit the completed document appropriately renamed as stated above;
- Lab exercise submission documents MUST be in Word 2003 or Word 2007 file formats that are NOT encoded in XML.

Discussion Threads

- Each course module includes a discussion topic that students are required to participate in. Student discussion postings will be graded as per the "Discussion Grading Rubric" under the Online Campus " Syllabus and Course Information" area.

Examinations

- Students are required to take six on-line quizzes (one per module) while the course is running. Students will be allowed 75 minutes to complete each quiz. A student may take each of these quizzes starting when a quiz becomes available via Online Campus. Each quiz will close at 6 AM ET on the date the next Module starts and not be reopened except for unusual circumstances as decided by the instructor. If a student cannot complete a quiz during the week each quiz is available, the student must make prior arrangements with the instructor.
- Students are required to take a proctored final exam that will last 3 hours. This exam is open book and open notes.
- A practice final exam will be available on Online Campus which can be taken as many times as a student wishes.
- If any work is to be completed beyond the scheduled dates of this course the student must negotiate a Boston University "Contract for an Incomplete Grade" with the professor prior to the end of the class.

Study Guide

Module 1 Study Guide and Deliverables	
Readings	Kaufman & Perlman Textbook Chapter 1 Sections 1.3 Terminology THROUGH 1.14 legal Issues The Blackboard material for this module The file Module 1 Example Company Security Policy - Extract.pdf The file Module 1 Network Overview and Review.pdf
Discussions	Make posts to Blackboard Discussion Board Discussion 1 Forum. Students are expected to create at least one new Discussion 1 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 1 via Blackboard Assignments by due date
Assessments	Complete and submit Quiz 1 via Blackboard Assessments by due date

Module 2 Study Guide and Deliverables	
Readings	Kaufman & Perlman Textbook Chapter 2, sections 2.1 What is Cryptography THROUGH 2.6 Hash Algorithms Chapter 3 sections 3.1 Introduction THROUGH 3.3.1 DES Overview 3.4 International Data Encryption Algorithm (IDEA) THROUGH 3.4.1 Primitive Operations 3.5 Advanced Encryption Standard (AES) 3.6 RC4 Chapter 4, sections 4.1 Introduction THROUGH 4.4.1.3 Triple Encryption with only Two Keys Chapter 6 sections 6.1 Introduction THROUGH 6.3.3 Why is RSA Secure 6.3.6 Public-Key Cryptography Standard (PKCS) 6.4 Diffie-Hellman THROUGH 6.4.2 Defenses Against Man-in-the-Middle Attack 6.4.5 Diffie-Hellman Details – Safe Primes 6.5 Digital Signature Standard (DSS) THROUGH 6.7 Elliptic Cure Cryptography (ECC) Chapter 9 sections 9.7.2 Certificate Authorities (CAs) THROUGH 9.7.4.2 Multiple CA Domains Chapter 15 sections 15.1 Introduction THROUGH 15.7 X.509 and PKIX Certificates Chapter 26 sections 26.1 Perfect Forward Secrecy THROUGH 26.2 Change Keys Periodically 26.4 Use Different Keys in the Two Directions THROUGH 26.24 Put Checksums at the End of Data The Blackboard material for this module
Discussions	Make posts to Blackboard Discussion Board Discussion 2 Forum. Students are expected to create at least one new Discussion 2 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 2 via Blackboard Assignments by due date
Assessments	Complete and submit Quiz 2 via Blackboard Assessments by due date

Module 3 Study Guide and Deliverables	
Readings	Kaufman & Perlman Textbook Chapter 5 sections 5.1 Introduction THROUGH 5.2 Nifty Things to Do with a Hash 5.2.1 Authentication THROUGH 5.2.4.1 Hashing Large Messages 5.5 MD5 5.6 SHA-1 THROUGH 5.6.1 SHA-1 Message Padding 5.7 HMAC Chapter 9 sections 9.1 Password-Based Authentication THROUGH 9..7.1 KDCs Chapter 10 sections 10.1 Introduction THROUGH 10.10 Biometrics Chapter 11 sections 11.1 Login THROUGH 11.8 Authentication Protocol Checklist Chapter 13 sections 13.1 Introduction THROUGH 13.6 Realms Chapter 16 sections 16.1 What Layer THROUGH 16.5 Denial-of-Service/Clogging Protection 16.12 Negotiating Crypto Parameters The Blackboard material for this module
Discussions	Make posts to Blackboard Discussion Board Discussion 3 Forum. Students are expected to create at least one new Discussion 3 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 3 via Blackboard Assignments by due date
Assessments	Complete and submit Quiz 3 via Blackboard Assessments by due date
Lab exercises	Complete and submit Lab 1 via Blackboard Assignments by due date
Module 4 Study Guide and Deliverables	
Readings	Kaufman & Perlman Textbook Chapter 17 sections 17.1 Overview of IPsec THROUGH 17.6 Comparison of Encodings Chapter 18 sections 18.1 Proturis THROUGH 18.6 Phase 2 IKE: Setting up IPsec SAs Chapter 23 sections 23.1 Packet Filters THROUGH 23.7 Should Firewalls Go Away The Blackboard material for this module
Discussions	Make posts to Blackboard Discussion Board Discussion 4 Forum. Students are expected to create at least one new Discussion 4 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 4 via Blackboard Assignments by due date
Assessments	Complete and submit Quiz 4 via Blackboard Assessments by due date
Lab exercises	Complete and submit Lab 2 via Blackboard Assignments by due date

Module 5 Study Guide and Deliverables	
Readings	Kaufman & Perlman Textbook Chapter 20 sections 20.1 Distribution Lists THROUGH 20.6 Authentication of the Source Chapter 22 sections 22.1 Introduction THROUGH 22.9 Anomalies Chapter 25 sections 25.1 Introduction THROUGH 25.6.6 Other Misuse of Cookie The Blackboard material for this module The file Module 5 A Review of Anomaly based Intrusion Detection Systems.pdf The file Module 5 Limitations of Network Intrusion Detection.pdf The file Module 5 Recent Advances and Future Trends in Honeypot Research.pdf The file Module 5 Honeypot in Network Security- A Survey.pdf The file Module 5 An Overview of IP Flow-Based Intrusion Detection.pdf
Discussions	Make posts to Blackboard Discussion Board Discussion 5 Forum. Students are expected to create at least one new Discussion 5 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 5 via Blackboard Assignments by due date
Assessments	Complete and submit Quiz 5 via Blackboard Assessments by due date
Lab exercises	Complete and submit Lab 3 via Blackboard Assignments by due date
Module 6 Study Guide and Deliverables	
Readings	The Blackboard material for this module The file Module 6 Guide to Computer Security Log Management.pdf The file Module 6 The design and implement of the centralized log gathering and analysis system.pdf The file Module 6 Log management comprehensive architecture in Security Operation Center.pdf The file Module 6 Technical Guide to Information Security Testing and Assessment.pdf
Discussions	Make posts to Blackboard Discussion Board Discussion 6 Forum. Students are expected to create at least one new Discussion 6 Forum Thread and post comments to Threads created by other students.
Assignments	Complete and submit Assignment 6 via Blackboard Assignments by due date
Assessments	Complete and submit Quiz 6 via Blackboard Assessment by due date

Student Submission Due Dates

- CS690 Student Submission dates are as follows:

	Submission Date & Time	Last Allowed **Late** Submission date
Assignment 1	9/25 at, or before, 6 AM ET	9/30 at, or before, 6 AM ET
Assignment 2	10/16 at, or before, 6 AM ET	10/21 at, or before, 6 AM ET
Assignment 3	10/30 at, or before, 6 AM ET	11/4 at, or before, 6 AM ET
Assignment 4	11/13 at, or before, 6 AM ET	11/18 at, or before, 6 AM ET
Assignment 5	11/27 at, or before, 6 AM ET	12/2 at, or before, 6 AM ET
Assignment 6	12/11 at, or before, 6 AM ET	Late not allowed
Quiz 1	9/25 at, or before, 6 AM ET	Late not allowed
Quiz 2	10/16 at, or before, 6 AM ET	Late not allowed
Quiz 3	10/30 at, or before, 6 AM ET	Late not allowed
Quiz 4	11/13 at, or before, 6 AM ET	Late not allowed

	Submission Date & Time	Last Allowed **Late** Submission date
Quiz 5	11/27 at, or before, 6 AM ET	Late not allowed
Quiz 6	12/11 at, or before,6 AM ET	Late not allowed
Discussion 1	9/25 at, or before, 6 AM ET	Late not allowed
Discussion 2	10/16 at, or before, 6 AM ET	Late not allowed
Discussion 3	10/30 at, or before, 6 AM ET	Late not allowed
Discussion 4	11/13 at, or before, 6 AM ET	Late not allowed
Discussion 5	11/27 at, or before, 6 AM ET	Late not allowed
Discussion 6	12/11 at, or before, 6 AM ET	Late not allowed
Lab Exercise 1	10/30 at, or before, 6 AM ET	11/4 at, or before, 6 AM ET
Lab Exercise 2	11/13 at, or before, 6 AM ET	11/18 at, or before, 6 AM ET
Lab Exercise 3	11/27 at, or before, 6 AM ET	12/2 at, or before, 6 AM ET

Grading Criteria

Students will have to do homework assignments to help you master the material. You will also have to read the textbooks and to be ready to discuss the issues related to the current class topics.

Grades will be based on:

- home work assignments (25%)
- quizzes (25%)
- lab exercises (10%)
- discussion thread participation (10%)
- proctored final exam (30%)

Grade ranges are as follows:

- 94 <= is an A
- 90 <= and < 94 is an A-
- 87 <= and < 90 is a B+
- 84 <= and < 87 is a B
- 80 <= and < 84 is a B-
- 77 <= and < 80 is a C+
- 74 <= and < 77 is a C
- 70 <= and < 74 is a C-
- 60 <= and < 70 is an F

Grades posted for un-proctored testing are contingent. They are confirmed if they are reasonably consistent with the grade on the final. In the case of inconsistency, students requesting confirmation must provide an explanation within a day of the release of their final grade.

Course Learning Objectives

Upon successful completion of this course students will be able to:

- Describe and correctly use the terminology and concepts associated with information security.
- Understand and be able to discuss the general concepts of information security governance.
- Understand and be able to discuss the importance of balancing the use of security policies, processes, technology and operations vs. costs to minimize organizational security risks.
- Develop detailed security requirements based on business needs, threat profiles, security policy obligations and asset vulnerabilities and exposure.
- Identify what type of protection different security services provide and which technical controls (e.g., symmetric/asymmetric encryption, cryptographically secure hash algorithms, key management approaches) are necessary to provide needed security services.
- Perform risk management activities, such as: asset assessments, determine probable threats and risks that drive solution architectural alternatives, trade-off studies, modeling and design issues.
- Describe and discuss security issues within general operating systems, specific commercial operating systems and application software
- Discuss the considerations when selecting appropriate anti-malware technologies.
- Describe and discuss security issues within common used network protocols and the approaches for mitigating communications associated threats.
- Prepare service/product security architectures and designs that sufficiently comply with enterprise security requirements thereby reducing risks to acceptable cost levels.
- Plan operational security procedures, ensure that operations security activities comply with policy, along with conducting periodic security reviews and audits.
- Support product and service development, integration and procurement activities ensuring that selected components, when deployed, will comply with the organization's detailed security requirements.

Course Outline

Module 1

Lecture 1 Why network security is needed, The different ways security is commonly discussed, Process of information security governance, The concept of defense in depth.

Lecture 2 – Foundation concepts: security services and controls Access control concepts, Asset inventory, classification concepts, vulnerabilities, threats and risks.

Module 2

Lecture 3 – Concept of encryption, Forms of symmetric and asymmetric encryption, cryptographically secure hash algorithms, impact of transmission bit errors on the use of encryption.

Lecture 4 – Encryption key attributes and cryptographic analysis. The need for encryption key management, key distribution approaches including Diffie-Hellman key negotiation, and Public Key Infrastructures.

Module 3

Lecture 5 - Role of Cryptography in Security to provide authentication, confidentiality and data integrity, The Extensible Authentication Protocol, Human Authentication and the concept of

Factors, Authentication Systems: Single Sign-on and XML, Kerberos and Shibboleth Based Authentication.

Lecture 6 – Traditional networking architectures, Types of networks (LANs, MANs, WANs), Network physical layer and data link layer attacks and defensive mechanisms available (IEEE 802.1ae, 802.1x).

Module 4

Lecture 7 – Additional Link Layer Protocols (PON, SONET MPLS, 802.15, 802.16 LTE). The Insecurity of ARP, IP and other network layer protocols covering vulnerabilities and protocol internal security mechanism.

Lecture 8 – Network layer attacks and defensive mechanisms available (IP security, packet filtering firewalls). Manets and SCADA networks considered

Module 5

Lecture 9 – Transport layer protocols, vulnerabilities, attacks and defensive mechanisms available (TLS-DTLS-SSL). Multi-protocols layer attacks and defensive mechanisms (Application gateway firewalls, Deep pack inspection).

Lecture 10 – Multi-protocols layer attacks and defensive mechanisms (network flow monitoring, Honey Pots). Web and Electronic mail vulnerabilities, attacks and defensive mechanisms (digest authentication, TLS, PGP-GPG).

Module 6

Lecture 11 – Malicious Software (Viruses, Worms, etc.). Applications for VoIP, Peer-to-peer, Instant Messaging and Peer-to-Peer networks/applications.

Lecture 12 – DHCP, Domain Name System, Network Time vulnerabilities, attacks and defensive mechanisms (Session Boarder Controls, DNS SEC, malware scanning)Security in management protocols**,** Network Security management tools (Syslog and log management, vulnerability scanning, Security Event and Information Management, Penetration Testing),

Lecture 13 – Network Operations Security (OpSec) and OpSec compliance.

Lecture 14 – Course review.

Non-required textbooks and references good for further study

The following books are **NOT** *required for this course. However you will find each to be valuable resources to anyone involved in the Information Security area.*

Bellovin, Addison-Wesley, 1994

This book is a classic for its very detailed treatment for statefull firewalls and DMZs and is still relevant today.

Practical UNIX & Internet Security, 2nd Edition, ,Simson Garfinkel and Gene Spafford: O'Reilly, 1996

This book is a classic for its very detailed treatment of general networking security and hardening of unix typs operating systems and is still relevant today.

Hacking Expose Network Security Secrets & Solutions, 2nd Edition, Joel Scambray, Stuart McClure, and George Kurtz, McGraw-Hill, 2001

This book provides an interesting look into those involved in malware and some of the techniques used for breaching targeted systems.

Security Engineering; A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, 2001

This book is an interesting collection of discussions on security engineering and associated challenges.

Computer Related Risks, Peter G. Neumann, Addison-Wesley, 1995

This book is one of the definitive texts on the basic concepts of what constitutes risks, especially information security risks.

Applied Cryptography, Bruce Schneier, 2nd Edition, Wiley & Sons, 1996

This book is an excellent source for details on most any encryption algorithm you are likely to encounter. Most any version, starting with the 2nd edition, will be invaluable.

Computer Security, Dieter Gollmann, 2nd ed, John Wiley, 2006

This book provides depth coverage of computer security and is highly recommended.

Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance, Stuart Jacobs, IEEE Press Series on Information and Communication Networks Security, Wiley-IEEE Press; 1 edition, ISBN-10: 0470565128, ISBN-13: 978-0470565124

The above book covers the subject area of information security from an engineering perspective