Enterprise Information Security

MET CS 695

Instructor

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

Office hours: By prior arrangement.

Office Address: 1010 Commonwealth Ave., Computer Science Dept., Boston, MA 02215.

E-mail: sjjacobs@bu.edu

Course Description

The goal of this course is to prepare students to perform security related tasks and contribute to organizational security related activities. Formal and technical aspects of information, computer and network security are presented and explained along with examples of real world systems, thereby enabling the student to relate theoretical approaches and both procedural and technical control implementations to meet the security requirements of enterprises.

The course provides an in-depth presentation of security issues in computer systems, networks, and applications. The concept of information security governance is presented and discussed. The basic concepts of security services, and the role played by encryption and hash algorithms are discussed along with issues and approaches for key management. Formal security models are explained and illustrated on operating system security aspects, more specifically memory protection, access control and authentication, file system security, backup and recovery management, intrusion and virus protection mechanisms. Application level security focuses on language level security and various security policies; conventional and public keys encryption, authentication, message digest and digital signatures. Internet and intranet topics include security in IP, routers, proxy servers, both packet filtering firewall and application-level gateway firewalls, Web servers, file and mail servers. Discussion of remote access issues, such as dial-up servers, modems, VPN gateways and clients are included.

Prerequisites

Knowledge of information technology fundamentals (computer hardware, operating systems, applications and networking) is required. Successful completion of CS 625, CS 535, or with **in advance** permission of the instructor.

Required Course Book

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; **2nd edition**, ISBN-13: 978-1119101604 ISBN-10: 1119101603

Courseware

This course uses Online Campus (Blackboard). Once the course starts all students must use the Online Campus Dashboard internal messages service. Students should **NOT** use the standard BU email system for course related emails. 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".

Required Hardware and Software

This course includes a number of student 'home' lab exercises. To complete these lab exercises, students will need access to:

- a laptop is required and running Windows 7, 8 or 10
  or
- a MAC with a virtualization program which runs Windows 10 like an app right on top of OS X or use Apple's built-in Boot Camp program to partition the hard drive to dual-boot Windows 10 right next to OS X.

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 (**9/4, 10/16, 11/13, 12/11** and the final exam on **12/19**) 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 134** at **808 Commonwealth Ave.**
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. For each day after the submission date a homework assignment is due will result in a penalty of 3 points. Homework assignments passed in that are over 5 days late will receive a grade of zero (0). If a student will be unable to submit an assignment by its due date, the student must contact the instructor **in advance** to avoid the late submission penalty.
   - 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. For each day after the submission date a lab exercise is due will result in a penalty of 3 points. Lab exercises passed in that are over 5 days late will receive a grade of zero (0). If a student will be unable to submit a Lab exercise by its due date, the student must contact the instructor **in advance** to avoid the late submission penalty.
   - 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.

   Unacceptable activities/behavior include 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, Study Guide, Lab Exercises & Examinations

Class Meetings

- The on-campus face-to-face class schedule for Fall 2017 MET CS 695 A1/E1 is:

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

Dates in this color and *italic* identify sessions where the B1 and E1 sections both meet on campus

On-line Live sessions

- There will be a number of one hour on-line sessions which will be held on the following Thursday evenings: 9/13, 9/20, 9/27, 10/11, 10/18, 10/25, 11/8, 11/15, 11/29, and 12/13 at 7:00 PM ET. During these on-line sessions I will be having a question & answer period. All on-line sessions will be recorded and archived. The archived recordings will be accessible from the Online Campus Dashboard under the heading "Live Classroom (Question & Answer) Sessions".

CS 695 Semester Meeting Times

- On the next page is a complete calendar for the fall 2018 that depicts the dates of all CS 695 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
9/3 Labor Day	9/4 **Class-1 joint** ***Module 1***	9/5	9/6	9/7	9/8	9/9
9/10	9/11 **Class-2**	9/12	9/13 On-line session 7pm	9/14	9/15	9/16
9/17	9/18 **Class-3** ***Module 2***	9/19	9/20 On-line session 7pm	9/21	9/22	9/23
9/24	9/25 **Class-4**	9/26	9/27 On-line session 7pm	9/28	9/29	9/30
10/1	10/2 **Class-5**	10/3	10/4	10/5	10/6	10/7
10/8 Columbus Day	10/9 no class	10/10	10/11 On-line session 7pm	10/12	10/13	10/14
10/15	10/16 **Class-6 joint** ***Module 3***	10/17	10/18 On-line session 7pm	10/19	10/20	10/21
10/22	10/23 **Class-7**	10/24	10/25 On-line session 7pm	10/26	10/27	10/28
10/29	10/30 **Class-8** ***Module 4***	10/31	11/1	11/2	11/3	11/4
11/5	11/6 **Class-9**	11/7	11/8 On-line session 7pm	11/9	11/10	11/11
11/12	11/13 **Class-10 joint** ***Module 5***	11/14	11/15 On-line session 7pm	11/16	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 On-line session 7pm	11/30	12/1	12/2
12/3	12/4 **Class-13**	12/5	12/6	12/7	12/8	12/9
12/10	12/11 **Class-14 joint**	12/12 Last day of classes	12/13 On-line session 7pm	12/14	12/15	12/16
12/17 Exam Start	12/18 **Final Exam**	12/19	12/20	12/21 Exam End	12/22	12/23

Assignments

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

  CS695-HW<number>-<student last name>.doc

  An example assignment document file name is: CS695-HW5-Jacobs.doc

  Student submissions which fail to follow this direction will have 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. If you cannot comply with this requirement, then you **MUST** contact me **in advance**. Student submissions which fail to follow this direction will have points deducted!
- 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.
  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. Please refer to the http://www.apastyle.org/ web site for guidance on following the APA style guide. Student submissions which fail to follow this direction will have points deducted!
- 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.

Papers to read prior to classes

Prior to Class 1 on 9/4 please read the following papers for in-class discussion

- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.
- Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. Security & Privacy, IEEE, 8(1), 21-27.

Prior to Class 6 on 11/16 please read the following papers for in-class discussion

- Robinette, G. J., & Marshall, J. S. (2001). An Integrated Approach to Risk Management and Risk Assessment. Incose Insight, 4(1), 23.
- Kalra, S., & Sood, S. K. (2011, July). Elliptic curve cryptography: survey and its security applications. In Proceedings of the International Conference on Advances in Computing and Artificial Intelligence (pp. 102-106). ACM.

Prior to Class 10 on 11/13 please read the following papers for in-class discussion

- Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. Wireless Communications, IEEE, 17(1), 51-58.
- Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. Smart Grid, IEEE Transactions on, 1(1), 99-107.

- Jacobs, S. (2012) Security Issues in Wireless Networks, Unpublished paper

Prior to Class 14 on 12/11 please read the following papers for in-class discussion

- Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011, May). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 96-111). IEEE.
- Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-A practical quantitative model. Journal of Research and Practice in Information Technology, 38(1), 45-56.

Study Guide

Module 1 Study Guide and Deliverables	
Readings	Engineering Information Security: Chapters 1 and 2. "Systems Engineering Fundamentals," Defense Acquisition University Press, 2001, chapters 1 through 13 (SEFGuide 01-01.pdf). Students are not expected to read this document in detail, but are expected to become familiar with what the document covers so they become aware of the document's value and possible applicability in their professional activities.
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
Lab exercises	There is no Lab Exercise for this module
Module 2 Study Guide and Deliverables	
Readings	Engineering Information Security: Chapters 3 and 4. Security Architecture for Open Systems Interconnection for CCITT Applications (ITU-T Recommendation X0800-91.pdf). Students are not expected to read this document in detail, but are expected to become familiar with what the document covers so they become aware of the document's value and possible applicability in their professional activities**.**
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
Lab exercises	There is no Lab Exercise for this module

Module 3 Study Guide and Deliverables	
Readings	Engineering Information Security: Chapters 5 and 6. DoD Trusted Computer System Valuation Criteria, sections 1.0 through 8.0 (DoD 5200-STD.pdf). Proposed NIST Standard for Role-Based Access Control, sections 1 through 6 (NIST Standard rbacSTD-ACM.pdf) Students are not expected to read these two documents in detail, but are expected to become aware of the documents' value and possible applicability in their professional activities**.**
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 exercise 1 – Windows Access Controls via Blackboard Assignments by due date
Module 4 Study Guide and Deliverables	
Readings	Engineering Information Security: Chapters 7 and 8.
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 exercise 2 – Scanning and Enumeration using Windows via Blackboard Assignments by due date
Module 5 Study Guide and Deliverables	
Readings	Engineering Information Security: Chapters 9 and 10.
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 exercise 3 - Windows Network Traffic Analysis via Blackboard Assignments by due date
Module 6 Study Guide and Deliverables	
Readings	Engineering Information Security: Chapters 11 and 12.
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 Assessments by due date
Lab exercises	There is no Lab Exercise for this module

Lab Exercises

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

  CS695-LAB<number>-<student last name>.doc

An example lab exercise document file name is:

CS695-LAB4-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. Student submissions which fail to follow this direction will have points deducted!

Student Submission Due Dates

- CS695 Student Submission dates are as follows:

	Submission Date & Time	Last Allowed **Late** Submission date
Assignment 1	9/18 at, or before, 5 PM ET	9/22 at, or before, 5 PM ET
Assignment 2	10/16 at, or before, 5 PM ET	10/20 at, or before, 5 PM ET
Assignment 3	10/30 at, or before, 5 PM ET	11/3 at, or before, 5 PM ET
Assignment 4	11/13 at, or before, 5 PM ET	11/17 at, or before, 5 PM ET
Assignment 5	11/27 at, or before, 5 PM ET	12/1 at, or before, 5 PM ET
Assignment 6	12/11 at, or before, 5 PM ET	Late not allowed
Quiz 1	9/18 at, or before, 5 PM ET	Late not allowed
Quiz 2	10/1 at, or before, 5 PM ET	Late not allowed
Quiz 3	10/30 at, or before, 5 PM ET	Late not allowed
Quiz 4	11/13 at, or before, 5 PM ET	Late not allowed
Quiz 5	11/27 at, or before, 5 PM ET	Late not allowed
Quiz 6	12/11 at, or before, 5 PM ET	Late not allowed
Discussion 1	9/18 at, or before, 5 PM ET	Late not allowed
Discussion 2	10/1 at, or before, 5 PM ET	Late not allowed
Discussion 3	10/30 at, or before, 5 PM ET	Late not allowed
Discussion 4	11/13 at, or before, 5 PM ET	Late not allowed
Discussion 5	11/27 at, or before, 5 PM ET	Late not allowed
Discussion 6	12/11 at, or before, 5 PM ET	Late not allowed
Lab Exercise 1	10/30 at, or before, 5 PM ET	11/3 at, or before, 5 PM ET
Lab Exercise 2	11/13 at, or before, 5 PM ET	11/17 at, or before, 5 PM ET
Lab Exercise 3	11/27 at, or before, 5 PM ET	12/1 at, or before, 5 PM ET

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 60 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 5 PM 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.
- All students are required to take a proctored final exam that will be held in class **on-campus** on

Tuesday **12/18** and last 3 hours. This exam is open book and open notes. Only the textbook will be allowed in electronic form during the final exam, all other materials MUST be in paper form.

- If the final will be missed it will be the responsibility of the student to arrange with the professor a mutually agreeable schedule for completion of work.
- A Practice Final Exam will be available on Online Campus which can be taken as many times as a student wishes. The purpose of the Practice Final exam is to allow students to prepare and practice for the actual graded Final Exam.
- 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.

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. n 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 Branches of security, Defining security by function, The Common Body of Knowledge (CBK) Security Domains, An example of security failures, Why every employee has a role in achieving information security, Introduction to security related terminology.

Lecture 2 - What is Systems Engineering: Stating the Problem, Investigate Alternatives and Model the System, Integrate, Launch the system, Assess performance, Re-evaluate, Process Variations. Process Management: ISO 9000 Processes and Procedures, Capability Maturity Model (CMM). Organization Environments: Regulations/Legislation, Technology Evolution, Customers demands and expectations, Legal Liability, Competition, Terrorism or Cyber crime. Business/Organizational Types: Commercial enterprises, Residential, Governmental, Non-Governmental Organizations (NGOs), National Critical Infrastructure

Module 2

Lecture 3 – Role of Cryptography in Information Security, Application of Services, Human Authentication and the concept of Factors, Cryptography, Cryptanalysis and Key Management.

Lecture 4 - Cryptographic Authentication, Authentication Systems: Kerberos Based Authentication, Public Key Infrastructures and human authentication.

Lecture 5 - Security policy development, security process management (governance) and associated standards, Security Policies, Risk management spanning assets, attack analysis and risk mitigation, Security requirements analysis and decomposition. Access control concepts, Security modeling and

security related standards.

Module 3

Lecture 6 – Traditional networking architectures, Types of networks (LANs, MANs, WANs), Network protocols, Data Link Layer complexity, The Insecurity of ARP, IP and the network Layer, Transport Protocols and protocol vulnerabilities and protocol internal security mechanisms

Lecture 7 – Next generation networking concepts and related security mechanisms.

Module 4

Lecture 8 - Generic security Related Hardware: Processor States and Status, Memory Addressing, Registers and Architectures, Interruption of Processor Activity, Operating Systems (OSs), The Security Kernel and Rings of protection, Memory and Address Protection, Fences, Relocation, Base/Bound Registers, Segmentation, Paging

Lecture 9 – Unix Type OS Security Capabilities. Solaris Security Capabilities and RBOC, Real-Time OS Security Capabilities, Microsoft Windows Security Capabilities. Applications software development security, malicious software (malware) and countermeasures.

Module 5

Lecture 10 - Layer 2 Network Security mechanisms (802.1q, 802.1x, 802.1i), Layer 3 Network Security mechanisms (IPsec, Firewalls, Intrusion Protection).

Lecture 11 - Layer 4 Network Security mechanisms (TLS, SSL, DTLS, SSH), Email Security

Module 6

Lecture 12 - Application Layer Network Security mechanisms (XML, SAML/IdM, VoIP & SBCs), Application Framework Security mechanisms (CORBA, DCE, Java, .NET, Active Directory).

Lecture 13 – .Security of Network Services (DNS, NTP), Penetration Testing, Network and Security management. Operational Security Compliance. Systems implementation, procurement and decommissioning.

Lecture 14 – Course review, student evaluations.

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.*

The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2nd edition, R.L. Krutz, and R. D. Vines, Wiley, 2004. ISBN: 0471413569
This book is very useful should you decide to sit for the CISSP examination to prepare you for the style and level of detail of questions in the six hour exam.

Firewalls and Internet Security, Repelling the Wily Hacker, William R. Cheswick, and Steven M. 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 type 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.

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