Information Security and Auditing in the Digital Age

A Practical and Managerial Perspective

Amjad Umar, Ph.D.

Publisher: NGE Solutions, Inc.
(www.ngesolutions.com)

Publication Date: Dec 2003

Umar, Amjad
Information Security and Auditing in the Digital Age, ISBN: 0-9727414-7-X

Publisher: NGE Solutions, Inc. (www.ngesolutions.com)

Author Website (www.amjadumar.com)

Book at a Glance

Trademark Acknowledgements

The following list recognizes the commercial and intellectual property of the trademark holders whose products are mentioned in this book. Omission from this list is inadvertant:

AIX is a trademark of IBM Corporation
CORBA is a trademark of Object Management Group
DB2 is a trademark of IBM Corporation
DCE is a trademark of Open Software Foundation
DSOM is a trademark of IBM Corporation
EDA/SQL is a trademark of Information Builders, Inc.
Encina is a trademark of IBM Corporation
Flowmark is a trademark of IBM Corporation
HotJava is a trademark of Sun Microsystems
IPX/SPX is a trademark of Novell Corporation
Java is a trademark of Sun Microsystems
J2EE, J2SE and J2ME are trademarks of Sun Microsystems
JSP and JDBC are trademarks of Sun Microsystems
Lotus Notes is a trademark of IBM Corporation
NetBIOS is a trademark of IBM Corporation
NetWare is a trademark of Novell Corporation
.Net is a trademark of Microsoft Corporation
ODBC is a trademark of Microsoft Corporation
OLE is a trademark of Microsoft Corporation
OpenMail is a trademark of Hewlett Packard
Orbix is a trademark of Iona Technologies
UNIX is a registered trademark licensed exclusively through X/Open Company, Ltd.
WebObjects is a trademark of NeXT Corporation
Windows is a trademark of Microsoft Corporation

Dedicated to my best friend – Dolorese -- who also happens to be my wife, fond memories of my parents and rest of the gang

Visit the Author Website (www.amjadumar.com) for:

- Additional information about this book and updates
- Purchasing options and instructions
- Instructor corner for course outlines, powerpoint slides, sample assignments
- Free slides (PDF format) of all chapters of the entire handbook that summarize the chapter topics and can be used as lecture notes
- Information about other books by the same author
- Frequently asked questions
- Feedback and suggestions
- Contacting the author
- Author background

PREFACE

This book provides a recent and relevant coverage based on a systematic approach. It was written to present a broad overview, with necessary details, of the following topics:

- Management issues of policies, procedures, risks, controls, and security requirements
- Practical review of security technologies such as cryptography, authentication, authorization, non-repudiation, and commercially available security packages (PKI, PGP, Kerberos, SSL, VPN)
- Securing wireless and wired networks by using the security technologies
- Securing enterprise applications, databases, and platforms by using the security technologies
- Examination of security risks associated with newer areas such as e-business, mobile applications, XML and Web Services, wireless communications, and application servers
- Audits and controls for continued secure operations
- A methodology that puts all of the above into a systematic procedure

Especially suitable for practitioners and managers, the book has also been classroom tested in IS/IT courses on security. The salient features of this classroom tested book are:

1. A security solutions approach that combines policies, procedures, risk analysis, threat assessment through attack trees, honeypots, and commercially available security packages to secure the modern IT assets as well as the paths (the wireless and wired networks) to these assets.

2. Broad coverage of recent and relevant topics such as the following based on a comprehensive framework:

- Application and database security with emphasis on modern issues such as e-commerce, e-business and mobile application security.
- Wireless security that includes security of Wi-Fi LANs, cellular networks, satellites, wireless home networks, wireless middleware,and mobile application servers.
- Semantic Web security with a discussion of XML security.
- Web Services security, SAML (Security Assertion Markup Language)and .NET security.
- Internet security (Public Internet, Intranet, Extranet),firewalls, remote access and perimeter security.

3. Integration of control and audit concepts in establishing a secure environment and continued compliance to a solution after deployment.

4. Practical discussion of security technologies (cryptography), authentication, authorization, accountability and availability with emphasis on intrusion detection, intrusion tolerance, and non-repudiation.

5. Case study orientation with numerous real-life examples and a single case study that is developed throughout the book to clarify and illustrate key points.

6. A mixture of management and technical issues for a balanced coverage of the topics.

7. Complete instructor materials (PowerPoint slides, course outline, project assignments) to support an academic or industrial course.

The book takes a total systems security solution view, shown in Figure 1, instead of one aspect. This view is the foundation of this book – the five blocks correspond to the five parts of this book (see "Book at a Glance" on a previous page and "Detailed Table of Contents" in the following pages for additional details):

- Part I presents detailed analysis of requirements and development of an overall approach.
- Part II concentrates on the examination and analysis of the most appropriate security technologies that are vital to a comprehensive solution.
- Part III and IV show how to protect the IT assets (the databases, applications, computers, and middleware) plus the access path (the wired and wireless network) to these assets by using the procedures and techniques discussed in Part I and II.

- Part V puts all the pieces together and concludes this book by showing how audits and controls can be established for continued secure operations.

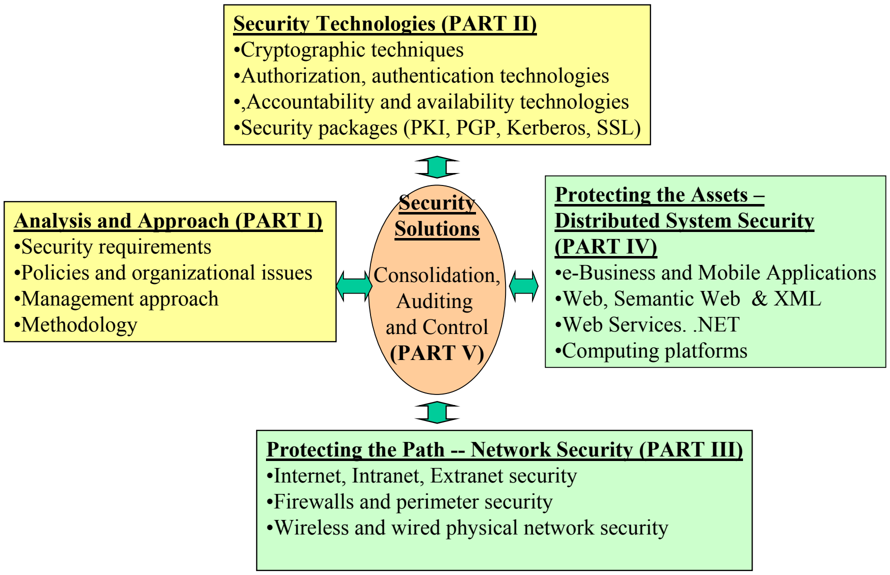

Security Technologies (PART II)
•Cryptographic techniques
•Authorization, authentication technologies
•,Accountability and availability technologies
•Security packages (PKI, PGP, Kerberos, SSL)
Analysis and Approach (PART I)
•Security requirements
•Policies and organizational issues
•Management approach
•Methodology
Security Solutions
Consolidation, Auditing and Control
(PART V)
Protecting the Assets – Distributed System Security (PART IV)
•e-Business and Mobile Applications
•Web, Semantic Web & XML
•Web Services. .NET
•Computing platforms
Protecting the Path -- Network Security (PART III)
•Internet, Intranet, Extranet security
•Firewalls and perimeter security
•Wireless and wired physical network security

Figure 1 : Total System Security View

Intended audience and recommended usage

The book was developed due to the knowledge gained in several industrial, research management, and university teaching assignments. The book can thus be used in academic courses, corporate training seminars, and as a self learning tool/reference guide. The intended audience is:

- IS managers who want to understand the recent and relevant information security issues and the approaches to address those issues.
- IS technical staff who need to analyze, develop, deploy, and/or live with the information security solutions in modern digital environments.
- IS and computer science students who want to get through a security course with minimal damage to their body and soul.
- All others who just want to read good books written by good people.

Conventions Used

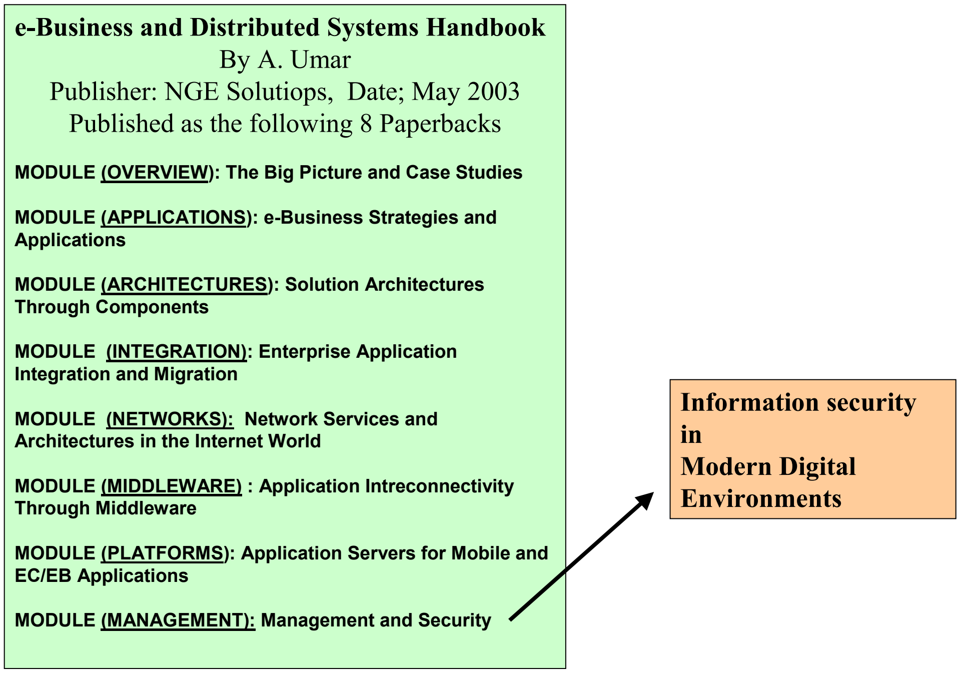
We will use the following conventions in this book. ***Highlighted italics*** are used to indicate definitions of new terms, *italics* are used for emphasis and **bold letters** are used for subject headings.

Acknowledgements

I am greatly indebted to my wife, Dolorese, who keeps supporting me through this endless writing process. This work could never have been finished without her help and understanding. Many thanks to my students at the University of Pennsylvania and Fordham University for "soldiering through" this material in various forms of readiness. Some interesting short case studies from some of these students appear in the book. I am also indebted to my colleagues and friends at Bellcore, now known as Telcordia Technologies, for exposing me to various security problems over past several years and for working with me through several projects in distributed systems, e-business, wireless systems, and security. Special thanks to Professor Aditya Saharia, Fordham Graduate School of Business, for supporting my course on information security at Fordham.

Relationship to e-Business and Distributed Systems Handbook

This book is in reality a spinoff from the “e-Business and Distributed Systems Handbook” that is published as 8 paperbacks (see Figure 2 and the sidebar “e-Business and Distributed Systems Handbook”). What is a spinoff book? The concept is similar to the TV spinoffs – one character (usually a support character) in a show becomes the main character in a spinoff. Some of us old timers remember Rhoda as a spinoff from the Mary Tyler Moore show and we all know the spinoffs from the successful CBS CSI show (CSI Miami, Navy CIS -- I do watch TV while writing all this stuff!). In the same vein, this book is a spinoff from the e-business handbook. In particular, it is a considerable expansion of the two security chapters that appeared in the Management Module of the handbook. Due to this, there is unavoidable overlap between the two chapters and this book. In addition, some modules of the handbook provide background that may be useful in this book (this book is written as a self contained work but some additional background about modern IT infrastructure may be needed by some readers).



e-Business and Distributed Systems Handbook
By A. Umar
Publisher: NGE Solutiops, Date; May 2003
Published as the following 8 Paperbacks

MODULE (OVERVIEW): The Big Picture and Case Studies

MODULE (APPLICATIONS): e-Business Strategies and Applications

MODULE (ARCHITECTURES): Solution Architectures Through Components

MODULE (INTEGRATION): Enterprise Application Integration and Migration

MODULE (NETWORKS): Network Services and Architectures in the Internet World

MODULE (MIDDLEWARE) : Application Intreconnectivity Through Middleware

MODULE (PLATFORMS): Application Servers for Mobile and EC/EB Applications

MODULE (MANAGEMENT): Management and Security

Information security in Modern Digital Environments

Figure 2: This Book is a Spinoff from the e-Business and Distributed Systems Handbook

e-Business and Distributed Systems Handbook

Amjad Umar (see **www.amjadumar.com** for details)

MODULE (OVERVIEW): The Big Picture and Case Studies
- Chapter 1: e-Business and Distributed Systems – From Strategies to Working Solutions
- Chapter 2: Case Studies and Examples

E-BUSINESS APPLICATIONS, ARCHITECTURES, AND INTEGRATION

MODULE (APPLICATIONS): e-Business Strategies and Applications
- Chapter 1: e-Business-- From Strategies to Applications
- Chapter 2: e-Business Applications (CRMs, ERPs, eMarkets, SCM, ASPs, Portals)
- Chapter 3: From Strategies to Solutions – A Planning Methodology
- Chapter 4: IT Infrastructure – Overview of Enabling Technologies
- Chapter 5: Applications State of the Practice, Market, and Art

MODULE (ARCHITECTURES): Solution Architectures Through Components
- Chapter 1: Solution Architecture Overview
- Chapter 2: Enterprise Application Architectures - A Component-based Approach
- Chapter 3: Enterprise Data Architectures in Web-XML Environments
- Chapter 4: Architecture Implementation: Concepts and Examples
- Chapter 5: Architectures State of the Practice, Market, and Art

MODULE (INTEGRATION): Enterprise Application Integration and Migration
- Chapter 1: Integration with Existing (Including Legacy) Applications -- An Overview
- Chapter 2: Enterprise and Inter-Enterprise Application Integration (EAI/eAI)
- Chapter 3: Data Warehouses and Data Mining for Integration
- Chapter 4: Migration Strategies and Technologies
- Chapter 5: Integration State of the Practice, Market, and Art

ENABLING IT INFRASTRUCTURE (NETWORKS AND MIDDLEWARE)

MODULE (NETWORKS): Network Services and Architectures in the Internet World
- Chapter 1: Principles of Communication Networks
- Chapter 2: Network Architectures and Interconnectivity
- Chapter 3: Wireless and Broadband Networks -- Next Generation Networks:
- Chapter 4: IP-based Networks and the Next Generation Internet
- Chapter 5: Networks State of the Practice, Market, and Art

MODULE (MIDDLEWARE) : Application Interconnectivity Through Middleware
- Chapter 1: Middleware Principles and Basic Middleware Services
- Chapter 2: Web, XML, Semantic Web, and Web Services
- Chapter 3: Distributed Objects, CORBA, Web Services, J2EE, .NET, SOAP, and EJB
- Chapter 4: Enterprise Data and Transaction Management
- Chapter 5: Middleware State of the Practice, Market, and Art

MODULE (PLATFORMS): Application Servers for Mobile and EC/EB Applications
- Chapter 1: Mobile Application Servers
- Chapter 2: e-Commerce Platforms for C2B Trade -- The Commerce Servers
- Chapter 3: B2B Platforms and Standards -- The B2B Servers
- Chapter 4: Platforms for Multimedia and Collaboration
- Chapter 5: Application Servers State of the Practice, Market, and Art

MANAGEMENT AND SUPPORT

MODULE (MANAGEMENT): Management and Security
- Chapter 1: e-Business Management in Practice
- Chapter 2: Management Platforms for Network and Systems Management
- Chapter 3: Security Management-- Approaches and Technologies
- Chapter 4: Security Solutions -- Using Technologies to Secure Systems
- Chapter 5: Management State of the Practice, Market, and Art

MODULE (TUTORIALS): Tutorials and Detailed Discussions on Special Topics
- Chapter 1: Network Technologies -- A Tutorial
- Chapter 2: Object-Orientation, Java, and UML -- A Tutorial
- Chapter 3: Database Technologies and SQL -- A Tutorial
- Chapter 4: Web Engineering and XML Processing -- A Closer Look
- Chapter 5: CORBA -- A Closer Look

Suggested Usage in a Course

This book has been classroom tested in different university and industrial courses in the past three years. These introductory courses were intended to provide a broad understanding of the subject matter that exposed the students to the managerial as well as technical aspects of security in the highly distributed environments in the digital age. The current book format has been largely influenced by the information security course that I taught in the Information and Communications Systems (ICS) department at Fordham Graduate School of business. The course was offered in the Fall 2003 Semester and was attended by MBA students, many of them practitioners in the IT industry.

The following course description outlines the course. I have taught variations of this course in the industry. The course can be easily modified for a more technical audience by adding one or two sessions on cryptographic techniques and by reducing/eliminating the management and audit/control topics. Conversely, more management focus can be provided by eliminating some of the technical topics in Part III and IV.

Information Security in the Digital Age; Sample Course Description

This course covers the technical as well as administrative aspects of security in modern digital enterprises from a total systems point of view instead of concentrating on one issue (e.g., network security, host security, data security, cryptography). The course starts with a comprehensive overview of security principles and practices that are needed to satisfy the IS systems integrity, confidentiality and availability requirements. The topics in this phase of the course include security awareness, security requirements, IS security and control practices, risk analysis, policies, and security management. A methodology for IS security is also introduced in this phase. The second part of the course covers the core security tools and techniques that are common to almost all security and audit practices. The topics in this phase of the course include: encryption based on symmetric/asymmetric techniques, authentication, access control, digital certificates, and digital signatures. Discussion also includes common security packages that combine these techniques into solutions such as PKI, PGP, SSL, and VPN. In the third phase, these techniques and methodology are used to build security solutions at an enterprise level. Topics in this phase cover Internet security, Web and Web Services security, XML security, application security, e-commerce security, wireless and mobile computing security, and other emerging cyber security issues. The course concludes with a discussion of information assurance in web environments, IT audit and control principles, and security audits needed for continued secure operations.

Course Objectives: Present a broad overview, with necessary details, of the following topics:

- Management issues of policies, procedures, risks, controls, and requirements
- Practical review of security technologies such as cryptography, authentication, authorization, non-repuduation, and commercially available security packages (PKI, PGP, Kerberos, SSL, VPN)
- Securing wireless and wired networks by using the security technologies
- Securing applications, databases, and platforms by using the security technologies
- Examination of security risks associated with newer areas such as e-business, mobile applications, XML and Web Services, wireless communications, and application server.
- Audits and controls for continued secure operations
- A methodology that puts all of the above into a procedure

Course Text

- Umar, A., "Information Security and Audits in the Digital Age", NGE Solutions, Dec. 2003

Additional main sources of Information

- Andress, M., "Surviving Security", SAMS Book, 2002 (recommended)

- "Guide to Information Technology, Control, and Audit", Frederick Gallegos (Editor), Sandra Allen-Senft, Daniel P. Manson
- Tipton, H. and Krause, M. editors, "Information Security Management Handbook", Auerbach, 2000
- Pipkin, D., Information Security: Protecting the Global Enterprise, Prentice Hall, 2000
- Schneier, B., *Secrets and Lies : Digital Security in a Networked World,* by John Wiley and Sons, 2004.
- Additional sources and web links made available during the course

Course Grade

Two projects (200 Points)
One Examination- Take home (100 Points)
Total: 300 points
Straight percentile grade

Course Outline

Legend:
U-Cn Umar, Chapter n

Phase 1: Introduction and EDP Audits

Session 1; Introduction to information security and audits (U-C1)
Session 2: : Security requirements, risk, and policies (U-C2)
Session 3: Security management and an overall methodology (U-C2,C3)

Phase 2: Security Principles and Technologies

Session 4: Cryptography techniques, symmetric/asymmetric encryption, digital signatures (U-C4)
Session 5: Authentication, authorization, accountability, availability, certificate management, non-repudiation, single sign-on (U-C5)
Session 6: Security packages (PKI, SSL, VPN, PGP, Kerberos) (U-C6)

Phase 3: Building Solutions to Secure IT Assets

Session 7; Review of IT assets, network security principles and firewalls (U-C7,C8)
Session 8; Internet security, VPNs/ IPSEC, Remote access security (U-C8)
Session 9: Wireless network security (U-C9)
Session 10: Web, Semantic Web, and XML security (U-C10)
Session 11: Distributed platform, Web Services, and .NET security (U-C11)
Session 12: Application security, e-commerce security, mobile application security (U-C12)
Session 13: Auditing and control, security audits (U-C13)
Session 14: Wrapup and Trends (U-C14)

Suggested Sample Projects

Projects are crucial to the learning experience. In the security courses I have taught, I have generally used two team projects (teams of 2-3 members) that include a mixture of research, hands-on experiments, and architectural analysis. Here is a sample list. You can pick any two or combine some of these to build larger team projects)

- Pick a security package, install it and do a demo of how it really works and how it can be used. Many students have used PGP due to its ready availability and have exchanged emails with each other by using PGP encryption. It works well. Examples of other packages are Kerberos, PKI and SSL. For

example, some students were able to obtain free trial digital certificates from Verisign and installed them on their browsers to experiment with various SSL options.
- Build a security solution for a sample company. The company is introduced in the early part of the project and then various security issues are addressed to develop a complete solutions. The book case study on NRW is an example and was in fact developed as student assignments. Instructors can extend this case study by adding additional capabilities to NRW that expose new threats to be addressed by a complete security solution. In many cases, the students chose a company that they are familiar with.
- Conduct a security audit of an actual or fictitious corporation. Many students have chosen parts of their organization or audited parts of university network, firewalls, etc.
- Research of special topics such as security policies, security audits, wireless security, e-commerce security, Web Services security, XML security, SAML, .NET security. controls for security, intrusion detection systems, non-repudiation, attack trees, honeypots, latest developments in cryptography, and many others. The material in this book serves as a good starting point. The main idea is to have students go beyond the classroom discussion and investigate the latest research and industrial developments. Students are asked to develop a proposal early in the term and make presentations on these topics and/or write a report.
- Programming assignments are especially useful pedagogical tools for students with adequate technical background. This is especially useful for the courses in computer science departments. Many security packages at present provide APIs that can be used to gain insights into system security. Students can, for example, build simple intrusion detection systems that detect intrusions caused by the students.

Detailed sample projects will be posted on the author website (www.amjadumar.com).

Acronyms and Glossary of Terms

ACL	Authorized control list
ACM	Association of Computing Machinery
ACSE	Association Control Service Elements
AI	Artificial Intelligence
AIA	Application Integration Architecture
API	Application Programming Interface
APPC	Advanced Program to Program Communications
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
ASP	Application service provider
ASP	Active Server pages – A Microsoft technology for building server side code
ATM	Asynchronous Transfer Mode – a packet switching technology used typically in high data rate networks
ATM	Automatic Teller Machine – used in banking
ATMF	Asynchronous Transfer Mode Forum
BISDN	Broadband Integrated Services Digital Network
BSP	Business System Planning
B2B	Business to business
B2C	Business to consumer
B2E	Business to employee
B2G	Business to government
CAD	Computer Aided Design
CAM	Computer Aided Manufacture
CBX	Computerized Branch Exchange
CCITT	Comité Consultatif Internationale de Télégraphique et Téléphonique (The International Telegraph and Telephone Consultative Committee)
CGI	Common Gateway Interface - A Web gateway technology
CICS	Customer Information Control System - an IBM mainframe transaction manager
CIM	Computer Integrated Manufacturing
CIO	Chief Information Officer
CLNP	Connectionless Mode Network Protocol
CLNS	Connectionless Mode Network Service
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
CMOT	Common Management Information Services and Protocol Over TCP/IP
CORBA	Common Object Request Broker Architecture
COTS	Commercial off-the-Shelf
CPU	Central Processing Unit
CRM	Customer Relationship management
CSF	Critical success factors
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
DAF/ODP	Distributed Application Framework/Open Distributed Processing
DAS	Distributed Application System
DBMS	Database Management System
DCP	Distributed Computing Platform
DCOM	Distributed Component Object Model

DCRM	Distributed Computing Reference Model
DCS	Distributed Computing System
DDBM	Distributed Database Manager
DDBMS	Distributed Database Management System
DDL	Data Definition Language – used in database management
DDTMS	Distributed Data and Transaction Management System
DFM	Distributed File Manager
DIS	Draft International Standard
DISOS	Distributed Operating System
DML	Data Manipulation Language
DNA	Digital Network Architecture
DOD	Department of Defense
DQDB	Distributed Queue Dual Bus
DRDA	Distributed Relational Database Architecture (from IBM)
DS	Directory Services
DSL	Digital subscriber loop
DTM	Distributed Transaction Manager
DTMS	Distributed Transaction Management System
EAI	Enterprise application integration
EB	Electronic Business
EC	Electronic commerce
EDI	Electronic Data Interchange
EJB	Enterprise Java Beans
ERP	Enterprise Resource Planning
ES-IS	End System to Intermediate System
ETSI	European Telecommunication Standards Institute
FAP	File Allocation Program (Procedure)
FDM	Frequency Division Multiplexing
FDDI	Fiber Distributed Data Interface
FEP	Front End Processor
FMS	Flexible Manufacturing System
FTAM	File Transfer, Access, and Management
FTP	File Transfer Protocol
GDMO	Guideline for Definition of Managed Objects
GUI	Graphical User Interface
IEEE	Institute for Electrical and Electronic Engineers
IDL	Interface Definition Language – used in CORBA and other distributed object middleware services
I/O	Input/Output
IMS	Information Management System - IBM DB/DC system on mainframes
IRM	Information resource management – a management methodology
IP	Internet protocol
IPC	Interprocess Communication
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet service provider
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Services Sector
JDBC	Java Database Connectivity
J2EE	Java Version 2 Enterprise Edition
PKI	Public key Infrastructure

LAN	Local Area Network
LDBMS	Local Database Management System
LLC	Logical Link Control
LU	Logical Unit - an endpoint in the IBM SNA environment
MAN	Metropolitan Area Network
MAC	Medium Access Control
MAP	Manufacturing Automation Protocol
Mbps	Million bits per second
MHS	Message Handling Service
MIB	Management information base - used in network management
MIPS	Million Instructions Per Second
MMS	Manufacturing Messaging Specification
MOM	Message oriented middleware
MVS	Multiple Virtual System - operating system on IBM's mainframes
MUX	Multiplexor
NAS	Network Application Support - DEC's open architecture
NBS	National Bureau of Standards
NCP	Network Control Program - a component of IBM's SNA
NFS	Network File Services - SUN Microsystem's File System for Networks
NIST	National Institute of Standards and Technology
NLM	Network Loadable Module (A Novell Netware feature)
NM	Network Management
NMF	Network Management Forum
NML	Network Management Layer
NMS	Network Management System
NOS	Network Operating Systems – typically indicates a LAN operating system (e.g., Novell Netware)
NSP	Network service provider (e.g., UUNET)
OAG	Open Application Group – a standards organization
ODBC	Open Database Connectivity – a de-facto standard for remote SQL
ODIF	Office Document Interchange Format
OEM	Original equipment manufacturer
OMG	Object Management Group
OODBMS	Object-Oriented Database Management System
OOPL	Object-Oriented Programming Language
OS	Operating System
OSF	Open Software Foundation
OSF-DCE	OSF Distributed Computing Environment
OSF-DME	OSF Distributed Management Environment
OSI	Open System Interconnection
OSS	Operations support systems - for telecom network provisioning
QoS	Quality of Service
QMP	Queued Message Processing
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PGP	Pretty Good Privacy
PU	Physical Unit - used in IBM's SNA
RDA	Remote Database Access
RTS	Reliable Transfer Service
RPC	Remote Procedure Call

SAA	System Application Architecture - IBM's "Open" Environment
SCM	supply chain managemnt
SDLC	Synchronous Data Link Control - Layer 2 Protocol in IBM's SNA
SET	Secure Electronic Transaction – a security standard
SIF	Synchronous Optical Network (SONET) Interoperability Forum
SQL	Structured Query Language
SMDS	Switched Muli-megabit Data Service
SML	Service-management layer - used in telecom network services
SNA	System Network Architecture - IBM's Network Architecture
SNMP	Simple Network Management Protocol - TCP/IP Network management Protocol
SOAP	Simple Object Activation Protocol – part of Web Services
SONET	Synchronous Optical Network
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TMN	Telecommunications managed network
TOP	Technical and Office Protocol
UDDI	Universal Description, Discovery and Integration - a registry for Web Services
UDP	User Datagram Protocol - a protocol that runs on IP
VAN	Value-added Network
VPN	Virtual Private Network
VT	Virtual Terminal
VTAM	Virtual Telecommunications Access Method - a component of IBM's SNA
VXML	Voice eXtensible Markup Language
WAN	Wide Area Network
WAP	Wireless Application Protocol
WML	Wireless Markup Language
WS	Workstation

Detailed Table of Contents

5 AUTHORIZATION, AUTHENTICATION, ACCOUNTABILITY, AND AVAILABILITY TECHNOLOGIES – THE 4 A'S

PART III: PROTECTING THE PATH –DIGITAL NETWORK SECURITY

7 OVERVIEW OF IT ASSETS IN MODERN DIGITAL ENTERPRISES

PART IV: PROTECTING THE SITES – DISTRIBUTED SYSTEM SECURITY

10 WEB, SEMANTIC WEB, AND XML SECURITY

11 MODERN DISTRIBUTED PLATFORM, WEB SERVICES AND .NET SECURITY

12 APPLICATIONS SECURITY: PROTECTING E-COMMERCE AND MOBILE APPLICATIONS