

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)
Copyright: 2003 by the Author

All Rights Reserved

No parts of this book may be reproduced without written permission of the author

Author Website (www.amjadumar.com)

Book at a Glance

PART I: ANALYSIS AND APPROACH

Chapter 1: Information Security in the Digital Age -- An Overview

Chapter 2: Security Management: Policies, Requirements, and Organizational Issues

Chapter 3: A Systematic Methodology: Linking People, Processes, and Technologies

PART II: THE SECURITY TECHNOLOGIES

Chapter 4: Cryptography and Encryption

Chapter 5: Authorization, Authentication, Accountability, and Availability Technologies – The 4As

Chapter 6: Common Security Packages: PKI, VPN, SSL, PGP and Kerberos

PART III: PROTECTING THE PATH –DIGITAL NETWORK SECURITY

Chapter 7: Overview of IT Assets in Modern Digital Enterprises

Chapter 8: Network Security, Internet Security, and Firewalls

Chapter 9: Wireless Security: Wifi, Cellular and Satellite Security

PART IV: PROTECTING THE SITES – DISTRIBUTED SYSTEM SECURITY

Chapter 10: Web, Semantic Web, and XML Security

Chapter 11: Modern Distributed Platform, Web Services and .NET Security

Chapter 12: Application Security: Protecting e-Commerce and Mobile Applications

PART V: PUTTING THE PIECES TOGETHER

Chapter 13: Audits and Controls for Security

Chapter 14: Building a Security Solution – The Wrapup

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 inadvertent:

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.

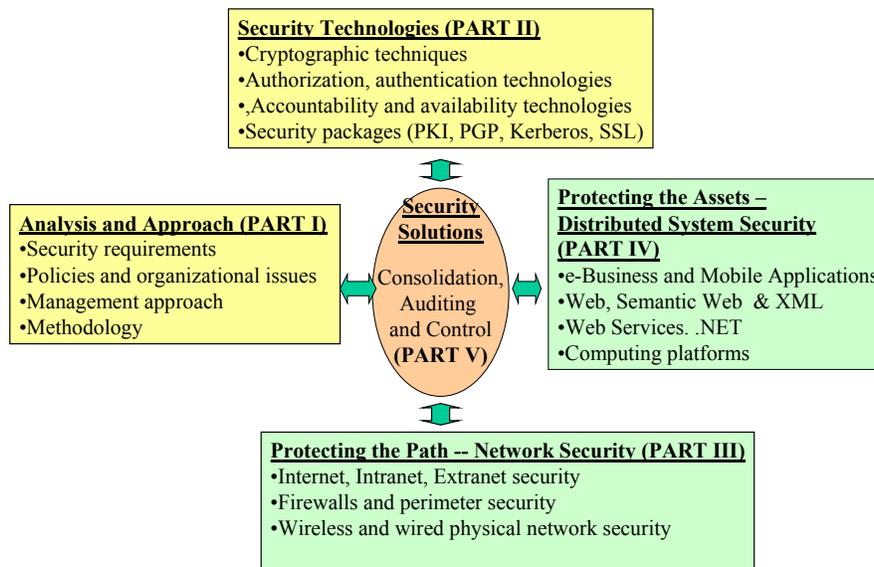


Figure 1 : Total System Security View

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, Dolores, 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).

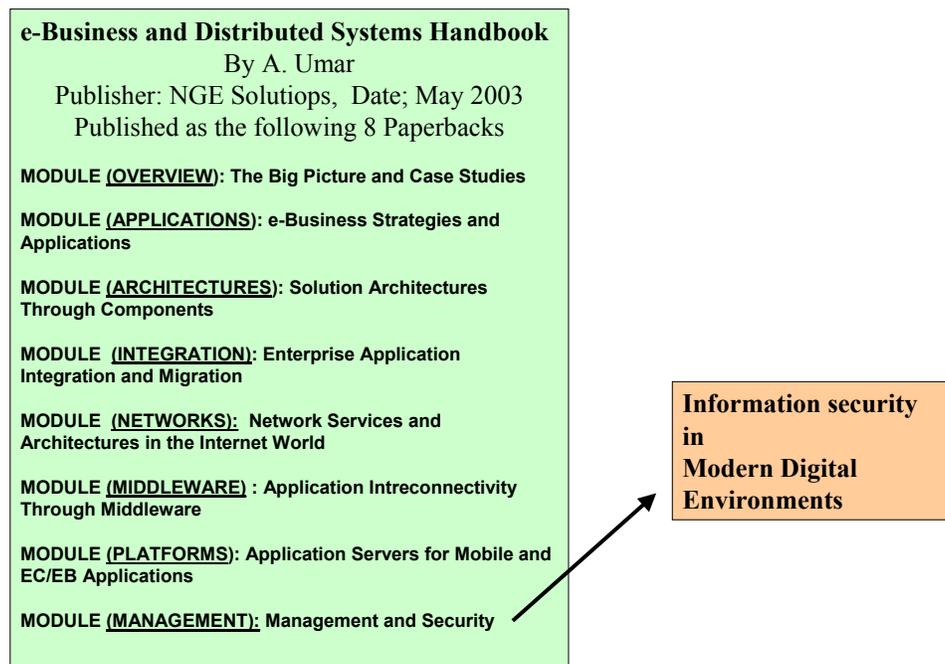


Figure 2: This Book is a Spinoff from the e-Business and Distributed Systems Handbook

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-Oriented, 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-repudiation, 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 Multi-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

PART I: ANALYSIS AND APPROACH

1 INFORMATION SECURITY IN MODERN ENTERPRISES – AN OVERVIEW

- 1.1 INTRODUCTION
- 1.2 SECURITY ISSUES UNIQUE TO THE DIGITAL AGE
 - 1.2.1 *The Vulnerabilities and Issues*
 - 1.2.2 *The IT Assets to be Protected*
- 1.3 EVOLUTION OF SECURITY -- THE DARPA VIEW AT A GLANCE
- 1.4 DEVELOPING SECURITY SOLUTIONS – A FRAMEWORK FOR DISCUSSION
 - 1.4.1 *Overview*
 - 1.4.2 *Analyzing Threats and Developing an Overall Approach*
 - 1.4.3 *Security Technologies at a Glance*
 - 1.4.4 *Securing the IT Assets and the Access Paths -- A Quick Glance*
 - 1.4.5 *Building and Deploying a Security Solution*
- 1.5 SECURITY IN ELECTRONIC COMMERCE – AN EXAMPLE
 - 1.5.1 *Overview*
 - 1.5.2 *Risk and Threat Analysis*
 - 1.5.3 *Analysis of Encryption Technologies*
 - 1.5.4 *Transmission Protection – Network Security*
 - 1.5.5 *Site Protection*
 - 1.5.6 *Security Solution, Audits and Controls*
- 1.6 SHORT CASE STUDIES OF SECURITY
 - 1.6.1 *Standard Chartered Bank: Remote Access Disaster Recovery/Business Continuity Plan*
 - 1.6.2 *CNN Denial of Service Attack*
 - 1.6.3 *Case Study: Power and Energy*
 - 1.6.4 *Analysis of IT Security in Pharmaceutical Trials*
- 1.7 CHAPTER SUMMARY
- 1.8 CONTINUING CASE STUDY: SECURITY FOR NERVOUS WRECK, INC. (NRW)
- 1.9 SUGGESTED REVIEW QUESTIONS

2 SECURITY MANAGEMENT: POLICIES, REQUIREMENTS, AND ORGANIZATIONAL ISSUES

- 2.1 INTRODUCTION
- 2.2 DEVELOPING POLICIES, CONTROLS, AND AUDITS
 - 2.2.1 *Developing Security Policies*
 - 2.2.2 *Short Case Study: Providing a Roadmap for IT Security by Using ISO 17799*
 - 2.2.3 *Establishing a Control Environment*
 - 2.2.4 *Audits for Evaluating Controls*
- 2.3 ORGANIZING AND TRAINING FOR SECURITY
 - 2.3.1 *Organizing for Security: Roles and Responsibilities*
 - 2.3.2 *Security Awareness*
 - 2.3.3 *Security Training*
 - 2.3.4 *Example: Government Agencies Beef Up IT Security*

- 2.4 ESTABLISHING SECURITY REQUIREMENTS
 - 2.4.1 *External Factors that Drive Security Requirements*
 - 2.4.2 *Organizational Requirements*
 - 2.4.3 *Tradeoffs between Security and Availability*
- 2.5 RISK AND VULNERABILITY MANAGEMENT
 - 2.5.1 *Risk Management*
 - 2.5.2 *Organizational Computing Models and Risks*
 - 2.5.3 *Security Trust Models and Risks*
 - 2.5.4 *Attack Trees for Analyzing and Mitigating Risks*
 - 2.5.5 *Automated Tools for Risk and Vulnerability Analysis*
- 2.6 DEVELOPING CIRCUMVENTIONS AND MITIGATING RISKS
 - 2.6.1 *Security Policies to Mitigate Risks*
 - 2.6.2 *Using Core Security Technologies for Circumventions*
- 2.7 SHORT CASE STUDIES -- PROTECTING THE IT ASSETS FROM INTERNAL ATTACKS
 - 2.7.1 *Global Retailer*
 - 2.7.2 *FBI*
 - 2.7.3 *Verizon*
 - 2.7.4 *Ethical and Organizational Issues in these Cases*
- 2.8 CHAPTER SUMMARY
- 2.9 REVIEW QUESTIONS AND EXERCISES

3 SECURITY METHODOLOGY: LINKING PEOPLE, PROCESSES, AND TECHNOLOGIES

- 3.1 INTRODUCTION
- 3.2 PUTTING THE PIECES TOGETHER – A METHODOLOGY
 - 3.2.1 *Overview*
 - 3.2.2 *Description of the Methodology*
 - 3.2.3 *Step 1: Develop Model of a System*
 - 3.2.4 *Step 2: Establish a Management Approach*
 - 3.2.5 *Step 3: Local Risk Analysis*
 - 3.2.6 *Step 4: Global Risk Analysis Through Attack Trees*
 - 3.2.7 *Step 5: Development of Countermeasures and Risk Mitigation*
 - 3.2.8 *Step 6: Updating System Designs*
 - 3.2.9 *Conclusions*
- 3.3 CONTINUING CASE STUDY: SECURITY FOR NRW (NERVOUS WRECK, INC.)
 - 3.3.1 *Overview*
 - 3.3.2 *Step 1: System Conceptual Model*
 - 3.3.3 *Step 2: Establish a Management Approach*
 - 3.3.4 *Step 3: Detailed Local Risk Analysis*
 - 3.3.5 *Step 4: Global Risk Analysis through Attack Trees*
 - 3.3.6 *Step 5: Choosing Enabling Security Technologies as Countermeasures*
- 3.4 CHAPTER SUMMARY
- 3.5 REVIEW QUESTIONS AND EXERCISES

PART II: THE SECURITY TECHNOLOGIES

4 CRYPTOGRAPHY AND ENCRYPTION

- 4.1 CRYPTOGRAPHY OVERVIEW

- 4.2 SYMMETRIC KEY ENCRYPTION -- THE CONVENTIONAL APPROACH
 - 4.2.1 *Overview*
 - 4.2.2 *Modern Cryptography Foundations*
 - 4.2.3 *Common Encryption Algorithms*
 - 4.2.4 *Issues with Symmetric (Secret) Key Cryptography*
- 4.3 PUBLIC KEY (ASYMMETRIC) CRYPTOGRAPHY
 - 4.3.1 *Overview*
 - 4.3.2 *Asymmetric Key Cryptography -- A Closer Look*
 - 4.3.3 *Symmetric Versus Asymmetric Cryptography*
 - 4.3.4 *Hybrid Encryption Systems*
- 4.4 SECURITY KEY CONSIDERATIONS: PERFORMANCE AND PROTECTION
- 4.5 DIGITAL SIGNATURES
 - 4.5.1 *Overview*
 - 4.5.2 *A Closer Look*
 - 4.5.3 *e-Signature Law*
- 4.6 MESSAGE DIGESTS FOR INFORMATION INTEGRITY
- 4.7 DIGITAL ENVELOPES -- COMBINING SYMMETRIC AND ASYMMETRIC KEY SYSTEMS
- 4.8 MAN IN THE MIDDLE – SECURITY WEAKNESS OF PUBLIC KEY SYSTEMS
- 4.9 EXAMPLES OF ENCRYPTION SYSTEMS
- 4.10 CONCLUDING COMMENTS: HOW SYMMETRIC AND ASYMMETRIC SYSTEMS ARE REALLY BEING USED IN PRACTICE
- 4.11 SHORT CASE STUDIES AND EXAMPLES
 - 4.11.1 *Legal Issues Concerning Publication of Encryption Algorithms*
 - 4.11.2 *Digital Signatures Support Mobile Home Banking*
 - 4.11.3 *Security in Health Care*
- 4.12 SUGGESTED REVIEW QUESTIONS

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

- 5.1 INTRODUCTION
- 5.2 AUTHENTICATION
 - 5.2.1 *Overview*
 - 5.2.2 *IDs and Passwords*
 - 5.2.3 *Token Cards: Secure ID, Smart Cards, and Java Rings*
 - 5.2.4 *Biometrics: Fingerprints, Eye Scans, and Speech Recognition*
 - 5.2.5 *Using Cryptography for Authentication – Digital Signatures and Session Keys*
 - 5.2.6 *Digital Certificates for Authentication*
 - 5.2.7 *Using Kerberos for Authentication*
 - 5.2.8 *Single Signon (SSO) Systems*
- 5.3 AUTHORIZATION AND INTRUSION DETECTION
 - 5.3.1 *Authorization and Access Controls*
 - 5.3.2 *Intrusion Detection*
 - 5.3.3 *Real-time Intrusion Detection Systems (IDSs)*
 - 5.3.4 *Data Mining for Intrusion Detection*
- 5.4 ACCOUNTABILITY AND NON-REPUDIATION
 - 5.4.1 *Overview*
 - 5.4.2 *Non-Repudiation – The Legal Meaning*
 - 5.4.3 *Non-Repudiation – The Crypto-Technical Meaning*
 - 5.4.4 *Technical Vulnerabilities for NR in Existing Systems*
 - 5.4.5 *Technologies and Approaches for Non-Repudiation*
- 5.5 AVAILABILITY AND INTRUSION TOLERANCE
 - 5.5.1 *High Availability – Dealing With Natural and Denial of Service Attacks*

- 5.5.2 *Denial of Service Attacks*
- 5.5.3 *High Availability, Fault Tolerance, and Intrusion Tolerance*
- 5.5.4 *Replication as a Backbone for Increased Availability*
- 5.5.5 *FRS (Fragmentation, Replication, Scattering)*
- 5.5.6 *Fragmentation Considerations*
- 5.5.7 *Scattering Considerations*
- 5.5.8 *Combining FRS with Cryptography*
- 5.5.9 *Special Considerations*
- 5.5.10 *The Reality Check on FRS*
- 5.6 SHORT CASE STUDIES AND EXAMPLES
 - 5.6.1 *Australian Agency Uses Digital Certificates to Sign Contract with Fujitsu*
 - 5.6.2 *How Computer-Savvy Investigators Operate*
 - 5.6.3 *City of Edmonton Upgrades Access Control*
- 5.7 CONCLUSIONS
- 5.8 SUGGESTED REVIEW QUESTIONS

6 COMMONLY USED SECURITY PACKAGES: PKI, VPN, SSL, PGP AND KERBEROS

- 6.1 INTRODUCTION
- 6.2 INTERRELATIONSHIPS BETWEEN TECHNOLOGIES, CONSUMERS, RESEARCHERS, AND SUPPLIERS
- 6.3 CERTIFYING AUTHORITIES AND THE PUBLIC KEY INFRASTRUCTURE (PKI)
 - 6.3.1 *What is PKI and Why is it Needed?*
 - 6.3.2 *Certifying Authorities (CAs)*
 - 6.3.3 *PKI Versus CA Services -- Practical Issues*
 - 6.3.4 *Entrust -- A Commercial PKI Product*
 - 6.3.5 *Verisign -- An Outsourcing Certificate Authority (CA)*
 - 6.3.6 *Players in PKI -- Standards and Technology Providers*
- 6.4 SECURE SOCKET LAYER (SSL) FOR WEB SECURITY
 - 6.4.1 *What is SSL*
 - 6.4.2 *How SSL Works*
- 6.5 VIRTUAL PRIVATE NETWORKS (VPNS) AND IPSEC
 - 6.5.1 *Virtual Private Networks (VPNs)*
 - 6.5.2 *IPSec*
- 6.6 PGP (PRETTY GOOD PRIVACY)
- 6.7 KERBEROS
- 6.8 OTHER PACKAGES AND CONCLUDING COMMENTS
- 6.9 SHORT CASE STUDIES AND EXAMPLES
 - 6.9.1 *Prudential/BT Managed PKI*
 - 6.9.2 *Global Public Key Infrastructure (PKI) for Least Developed Countries*
 - 6.9.3 *Utilities Choose PGP Encryption Over S/MIME*
- 6.10 SUGGESTED REVIEW QUESTIONS
- 6.11 PART II -- NRW CASE STUDY REVISITED: CHOOSING ENABLING SECURITY TECHNOLOGIES AS COUNTERMEASURES

PART III: PROTECTING THE PATH--DIGITAL NETWORK SECURITY

7 OVERVIEW OF IT ASSETS IN MODERN DIGITAL ENTERPRISES

- 7.1 INTRODUCTION
- 7.2 NETWORK SERVICES AND THE INTERNET
 - 7.2.1 *Overview of Network Services*
 - 7.2.2 *Network Interconnectivity*
 - 7.2.3 *Broadband and Wireless Networks*
 - 7.2.4 *IP Networks and the Internet*
 - 7.2.5 *Private Value Added Networks (VANs).*
 - 7.2.6 *Extranets and Virtual Private Networks (VPNs)*
- 7.3 COMPUTING PLATFORMS -- OPERATING SYSTEMS AND LOCAL SYSTEMS SOFTWARE
 - 7.3.1 *Operating Systems*
 - 7.3.2 *Local Systems Software*
- 7.4 GENERAL PURPOSE MIDDLEWARE
 - 7.4.1 *Overview*
 - 7.4.2 *Basic Client/Server Middleware*
 - 7.4.3 *Web and XML*
 - 7.4.4 *Distributed Objects for Enterprise Wide Applications*
 - 7.4.5 *Distributed Transaction Support*
- 7.5 HIGHER LEVEL MIDDLEWARE AND APPLICATION SUPPORT PLATFORMS
 - 7.5.1 *Middleware for Mobile Computing and Wireless Networks*
 - 7.5.2 *Enterprise Application Integrators (EAI) and Message Brokers*
 - 7.5.3 *Middleware to Support E-commerce*
 - 7.5.4 *Electronic Commerce Platforms: Packaging EC Middleware*
 - 7.5.5 *Platforms for Application Development and Deployment -- The Application Servers*
- 7.6 3G DISTRIBUTED COMPUTING ENVIRONMENTS (DOT NET AND J2EE)
 - 7.6.1 *Sun J2EE*
 - 7.6.2 *Microsoft's Dot Net*
- 7.7 PUTTING THE PIECES TOGETHER -- AN EXAMPLE
- 7.8 CASE STUDY: OPEN SOURCE-BASED INFRASTRUCTURE
- 7.9 SUMMARY
- 7.10 REVIEW QUESTIONS AND EXERCISES

8 NETWORKS SECURITY, INTERNET SECURITY AND FIREWALLS

- 8.1 INTRODUCTION
- 8.2 PHYSICAL NETWORK SECURITY
 - 8.2.1 *Overview*
 - 8.2.2 *LAN Access Security*
 - 8.2.3 *A Note about Hub versus Switch Security*
 - 8.2.4 *Remote Access Security -- General Considerations*
 - 8.2.5 *Dial-Up Network Security*
 - 8.2.6 *AAA Servers and Remote Access Dial-in User Service (RADIUS)*
- 8.3 PUBLIC INTERNET SECURITY
 - 8.3.1 *The Public Internet at a Glance*
 - 8.3.2 *Public Internet Security Issues*
 - 8.3.3 *ISPs and NSPs as Players in the Public Internet Security*
 - 8.3.4 *Internet Security Through VPNs and IPSec*
- 8.4 CORPORATE INTRANET AND EXTRANET SECURITY
 - 8.4.1 *Overview of Corporate Network Security Issues*
 - 8.4.2 *What are Intranets and Extranets?*
 - 8.4.3 *Corporate Intranet and Extranet Architectures for Security*
- 8.5 FIREWALLS -- PROTECTING THE ENTERPRISE PERIMETER
 - 8.5.1 *Overview*
 - 8.5.2 *Firewall Configurations*

- 8.5.3 *Firewall Administration, Design Issues and Policies*
- 8.6 SHORT CASE STUDIES AND EXAMPLES
 - 8.6.1 *Combining Network and Physical Security*
 - 8.6.2 *beBetter Networks Chooses a FireWall*
 - 8.6.3 *Secure Automated Change Management for a University Network*
 - 8.6.4 *From Site Finder to Internet Ownership*
 - 8.6.5 *Using SATAN to Reduce Network Security Exposures*
 - 8.6.6 *Digital Networks Tie Together National and Local Security*
- 8.7 SUGGESTED REVIEW QUESTIONS BEFORE PROCEEDING

9 WIRELESS SECURITY: WIFI, CELLULAR AND SATELLITE SECURITY

- 9.1 INTRODUCTION
- 9.2 OVERVIEW OF WIRELESS NETWORKS AND WIRELESS SECURITY
 - 9.2.1 *Wireless Networks at a Glance*
 - 9.2.2 *A Quick Overview of Wireless Security*
- 9.3 WIRELESS LAN SECURITY
 - 9.3.1 *Overview*
 - 9.3.2 *The Wireless Ethernet (802.11) LANs*
 - 9.3.3 *Wireless Ethernet (802.11) Security Issues*
 - 9.3.4 *Wired Equivalent Privacy (WEP)*
 - 9.3.5 *IEEE 802.1X "Network Port Authentication"*
 - 9.3.6 *802.11 Wireless Roaming*
 - 9.3.7 *Approaches to Secure WLANs*
- 9.4 WIRELESS PERSONAL AREA NETWORK SECURITY
 - 9.4.1 *Overview*
 - 9.4.2 *Cordless Phone and Home RF Security*
 - 9.4.3 *Bluetooth Security*
- 9.5 CELLULAR WIRELESS NETWORK SECURITY
 - 9.5.1 *Overview*
 - 9.5.2 *Cellular Network Security Solution Approaches*
- 9.6 SATELLITE SECURITY
 - 9.6.1 *Overview*
 - 9.6.2 *Approaches to Secure Satellite Communications*
- 9.7 WIRELESS LOCAL LOOP (WLL) SECURITY
- 9.8 EMERGING WIRELESS NETWORK SECURITY
 - 9.8.1 *Overview*
 - 9.8.2 *Free Space Optics (FSO) Security*
 - 9.8.3 *UWB Security*
 - 9.8.4 *Mobile Ad Hoc Network Security*
- 9.9 MOBILE IP SECURITY
- 9.10 WIRELESS MIDDLEWARE SECURITY
 - 9.10.1 *Overview*
 - 9.10.2 *Secure Socket Layer (SSL) for Wireless Web Security*
 - 9.10.3 *WAP Security and WTLS*
 - 9.10.4 *I-Mode Security*
 - 9.10.5 *Wireless VPN Versus WAP Security*
- 9.11 SHORT EXAMPLES AND CASE STUDIES
 - 9.11.1 *Wireless in Government Services*
 - 9.11.2 *Wireless Security in the Health Sector*
 - 9.11.3 *Wireless LANs at Texas A&M University*
- 9.12 SUMMARY AND CONCLUSIONS

- 9.13 SUGGESTED REVIEW QUESTIONS
- 9.14 REFERENCES FOR WIRELESS SECURITY
- 9.15 PART III - NRW CASE STUDY REVISITED: SECURING WIRELESS AND WIRED NETWORKS
 - 9.15.1 *Overview*
 - 9.15.2 *Detailed Physical Model for Wireless and Wired Network Security Analysis*
 - 9.15.3 *Analyze Security Risks*
 - 9.15.4 *Develop Countermeasures*

PART IV: PROTECTING THE SITES – DISTRIBUTED SYSTEM SECURITY

10 WEB, SEMANTIC WEB, AND XML SECURITY

- 10.1 INTRODUCTION
- 10.2 TRADITIONAL WEB SECURITY AND SSL
 - 10.2.1 *General Web Security Considerations*
 - 10.2.2 *Secure Socket Layer (SSL) for Web Security*
 - 10.2.3 *S-HTTP (Secure HTTP)*
 - 10.2.4 *Web Cookies -- Some Privacy Issues*
 - 10.2.5 *Web Proxies for Security*
- 10.3 SEMANTIC WEB AND SEMANTIC WEB SECURITY
 - 10.3.1 *Overview of Semantic Web*
 - 10.3.2 *XML -- A Quick Overview*
 - 10.3.3 *XML Security, XML Encryption and XML Signature*
 - 10.3.4 *The "XML-ing" of PKI: ;;; FROM GARTNER, REPHRASE, ETC,*
 - 10.3.5 *Web Metadata and PICS (Platform for Internet Content Selection)*
 - 10.3.6 *Platform for Privacy Preferences (P3P)*
 - 10.3.7 *Resource Definition Framework (RDF) and RDF Security*
 - 10.3.8 *Document Object Model (DOM) and DOM Security*
- 10.4 SHORT CASE STUDIES AND EXAMPLES
 - 10.4.1 *Web Security at Exostar*
 - 10.4.2 *Jitux.A Worm Targets MSN Messenger Users*
 - 10.4.3 *A Global Financial Services Company Uses XML Signature*
- 10.5 SUGGESTED REVIEW QUESTIONS

11 MODERN DISTRIBUTED PLATFORM, WEB SERVICES AND .NET SECURITY

- 11.1 INTRODUCTION
- 11.2 OPERATING SYSTEM AND LOCAL SOFTWARE SECURITY -- A QUICK OVERVIEW
 - 11.2.1 *Operating System (OS) Security*
 - 11.2.2 *Server Hardening*
 - 11.2.3 *Database and Transaction Security*
 - 11.2.4 *Host Resident Firewalls*
- 11.3 MIDDLEWARE SERVICES SECURITY
 - 11.3.1 *Introduction*
 - 11.3.2 *Middleware and Middleware Platforms -- A Revisit*
 - 11.3.3 *Basic Middleware Security and Secure RPCs*
 - 11.3.4 *CORBA Security*
 - 11.3.5 *e-Commerce (EC) Platform Security*
 - 11.3.6 *Mobile Application Server (MAS) Security*
 - 11.3.7 *EAI (Enterprise Application Integration) Security*
- 11.4 WEB SERVICES SECURITY AND SAML
 - 11.4.1 *Overview of Web Services*

- 11.4.2 *Issues Unique To Web Services Security*
- 11.4.3 *Web Services Security Approaches*
- 11.4.4 *SAML (Security Assertion Markup Language)*
- 11.4.5 *Web Services Security Summary*
- 11.5 .NET SECURITY
 - 11.5.1 *Overview of .NET*
 - 11.5.2 *.NET Security – Main Feature*
 - 11.5.3 *.NET Passport -- A Possible Solution for Single Signon*
- 11.6 SHORT CASE STUDIES AND EXAMPLES
 - 11.6.1 *Web Services Security by Using a Firewall*
 - 11.6.2 *Microsoft .NET Security at Wakefield Public Schools*
 - 11.6.3 *Microsoft .NET Passport Helps Student Loans*
- 11.7 REVIEW QUESTIONS

12 APPLICATIONS SECURITY: PROTECTING E-COMMERCE AND MOBILE APPLICATIONS

- 12.1 INTRODUCTION
- 12.2 DISTRIBUTED APPLICATION PROTECTION – GENERAL CONSIDERATIONS
 - 12.2.1 *Overview*
 - 12.2.2 *Tradeoffs between Application and Lower Level Security Issues*
 - 12.2.3 *Client Side Security*
 - 12.2.4 *Web Server Tier (Middle Tier) Security*
 - 12.2.5 *Web Services Security and SAML (Security Assertion Markup Language)*
 - 12.2.6 *Back-end System Security – Protecting the Legacy Systems*
- 12.3 BASIC E-COMMERCE SECURITY AND SET
 - 12.3.1 *Why e-Commerce Security is important*
 - 12.3.2 *Online Purchasing Security Through SET*
 - 12.3.3 *Weak Server-Side Programs -- The main Weakness of e-Commerce Security*
- 12.4 E-BUSINESS APPLICATIONS SECURITY
 - 12.4.1 *Overview*
 - 12.4.2 *Consumer to Business (C2B) Applications Security*
 - 12.4.3 *B2E Internal Business Applications -- The ERPs (Enterprise Resource Planning)*
 - 12.4.4 *Business-to-Business (B2B): Supply Chain and eMarket Security*
 - 12.4.5 *Consumer to Data (C2D) Applications -- Business Intelligence*
 - 12.4.6 *Consumer to Consumer (C2C) Applications - Collaborative Computing and Groupware*
- 12.5 MOBILE APPLICATION AND MOBILE COMMERCE SECURITY
 - 12.5.1 *Overview*
 - 12.5.2 *Mobile Applications Issues*
 - 12.5.3 *Mobile Client Security*
- 12.6 MOBILE AGENT SECURITY
 - 12.6.1 *Overview*
 - 12.6.2 *Sample Applications of Mobile Agents in Ecommerce*
 - 12.6.3 *Generic Architecture of Mobile Agent Environments*
 - 12.6.4 *Security Issues in Mobile Agents*
 - 12.6.5 *Mobile Agent Security Summary*
- 12.7 EMAIL SECURITY -- S/MIME AND PGP
- 12.8 ADDITIONAL APPLICATION SECURITY ISSUES
- 12.9 MALICIOUS PROGRAMS AND VIRUSES
 - 12.9.1 *Overview*
 - 12.9.2 *Common Means of Introducing Malicious Code*
 - 12.9.3 *What Can Be Done?*

- 12.10 SHORT CASE STUDIES AND EXAMPLES
 - 12.10.1 *Centex Avoids the Nimda Worm*
 - 12.10.2 *e-Business Security at an International Financial Institution*
 - 12.10.3 *Yellow Corporation Detects Intrusions in its eBusiness Operations*
- 12.11 SUGGESTED REVIEW QUESTIONS
- 12.12 PART IV CASE STUDY REVISITED: NRW ADOPTS WEB SERVICES AND MOBILE APPLICATIONS
 - 12.12.1 *Overview*
 - 12.12.2 *Risk Analysis*
 - 12.12.3 *Risk Mitigations and Circumventions*

PART V: PUTTING THE PIECES TOGETHER

13 AUDITS AND CONTROLS FOR SECURITY

- 13.1 INTRODUCTION
- 13.2 ESTABLISHING A CONTROL ENVIRONMENT
 - 13.2.1 *Overview*
 - 13.2.2 *Application Controls*
 - 13.2.3 *IT Infrastructure Controls*
 - 13.2.4 *Administrative and Process Controls*
 - 13.2.5 *Costs and Benefits of Controls*
 - 13.2.6 *Audits for Evaluating Controls*
- 13.3 SECURITY AUDITS – THE BIG PICTURE
 - 13.3.1 *Introduction*
 - 13.3.2 *Management Considerations in Security Audits*
 - 13.3.3 *Security Policy as a Basis for Audits*
 - 13.3.4 *Audit as an On-Going Process*
- 13.4 PREPARING AND PLANNING FOR A SECURITY AUDIT
 - 13.4.1 *Setting Scope of the Audit*
 - 13.4.2 *Gathering Information and Review of Documents*
 - 13.4.3 *Develop an Audit Plan and Choose Tools*
- 13.5 EXECUTING A SECURITY AUDIT
 - 13.5.1 *Getting Started*
 - 13.5.2 *Interviews*
 - 13.5.3 *Technical Investigations*
 - 13.5.4 *The Tools*
- 13.6 CONCLUDING AN AUDIT – PREPARING THE AUDIT REPORT
 - 13.6.1 *Consolidating and Analyzing the Results*
 - 13.6.2 *The Audit Report*
- 13.7 CASE STUDY -- SECURITY AUDIT FOR THE FISH.COM NETWORK
 - 13.7.1 *Executive Summary*
 - 13.7.2 *Security Policies and Documentation*
 - 13.7.3 *Network Security*
 - 13.7.4 *Security Architecture and Design*
 - 13.7.5 *Host Security*
 - 13.7.6 *Physical Security*
- 13.8 SUGGESTED REVIEW QUESTIONS AND EXERCISE

14 BUILDING A SECURITY SOLUTION – THE WRAPUP

14.1 PUTTING THE PIECES TOGETHER -- BUILDING A SECURITY SOLUTION

14.1.1 Overview

14.1.2 Establishing a Solution Architecture

14.1.3 Intrusion Threats Due to Networks

14.1.4 Intrusion Threats Due to Middleware

14.1.5 Intrusion Threats for Applications

14.1.6 Evaluating Security Versus Availability

14.2 CHEATING THE CHEATERS -- HONEYPOTS AND OTHER DIVERSIONS

14.2.1 What are Honeypots?

14.2.2 Types of Honeypots

14.2.3 Production Honeypots

14.2.4 Experimental and Research Honeypots

14.2.5 Commercially Available Honeypots and Issues with Honeypots

14.3 WRAPUP -- SECURITY SOLUTION FOR NRW

14.4 CHAP 14 -- WRAPUP -- SECURITY SOLUTION FOR NRW

14.5 SUMMARY AND CONCLUSIONS