Fundamentals of Information Systems Security

Lesson 12

Information Security Standards

Learning Objective(s)

- Apply information security standards and U.S. compliance laws to real-world applications in both the private and public sector.

Key Concepts

- International information security standards and their impact on IT infrastructures
- ISO 17799
- ISO/IEC 27002
- Payment Card Industry Data Security Standard (PCI DSS) requirements

Information Security Standards

Necessary to create and maintain a competitive market for hardware and software vendors

Guarantee compatibility between products from different countries

Provide guidelines to ensure that products in today's computing environments work together

Standards Organizations

- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- World Wide Web Consortium (W3C)
- Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Telecommunication Union Telecommunication Sector (ITU-T)
- American National Standards Institute (ANSI)
- ETSI Cyber Security Technical Committee (TC CYBER)

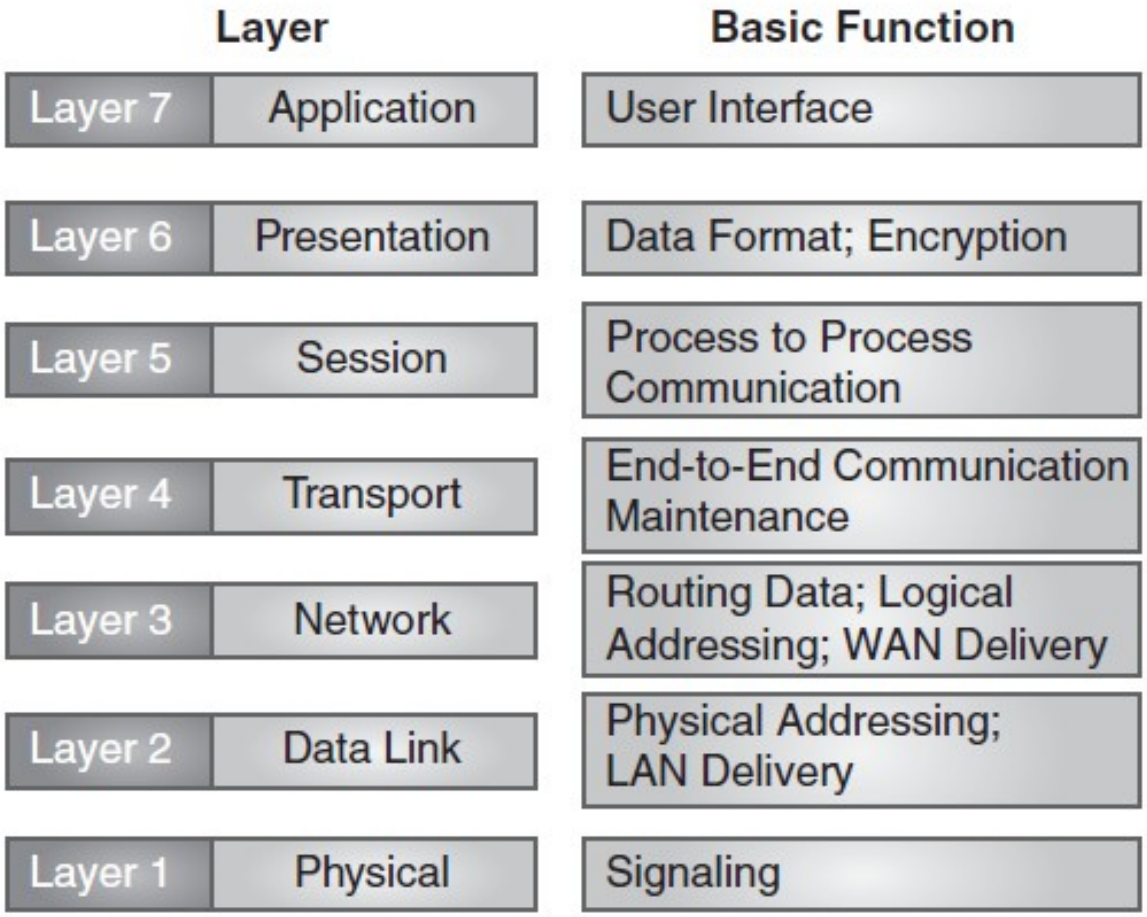
National Institute of Standards and Technology (NIST)

- Federal agency within the U.S. Department of Commerce
- Mission is to “promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life”
- Provides standards for measurement and technology on which nearly all computing devices rely
- Maintains the atomic clock that keeps the United States’ official time
- Maintains a list of standards and publications of general interest to the computer security community

International Organization for Standardization (ISO)

- Nongovernmental international organization
- Its goal is to develop and publish international standards for nearly all industries
- Is a network of 161 national standards institutes
- Serves as a bridge between the public and private sectors
- Best-known ISO standard is the Open Systems Interconnection (OSI) Reference Model

The OSI Reference Model



International Electrotechnical Commission (IEC)

Works with the ISO

Is the preeminent organization for developing and publishing international standards for technologies related to electrical and electronic devices and processes

Standards address a wide variety of areas

- Power generation
- Semiconductors
- Telecommunications
- Physical computer and networking hardware

World Wide Web Consortium (W3C)

Is the main international standards organization for the World Wide Web

Develops protocols and guidelines that unify the Web and ensure its long-term growth

Standards developed or endorsed include:

- Cascading Style Sheets (CSS)
- HyperText Markup Language (HTML)
- Simple Object Access Protocol (SOAP)
- Extensible Markup Language (XML)

Internet Engineering Task Force (IETF)

- Develops and promotes Internet standards
- Focuses on the engineering aspects of Internet communication
- Works closely with the W3C and ISO/IEC
- Is a collection of working groups (WGs), with each group addressing a specific topic

Request for Comments (RFC)

- A document that ranges from a simple memo to several standards documents
- RFC model allows input from many sources; encourages collaboration and peer review
- Only some RFCs specify standards
- RFCs never change
- RFCs may originate with other organizations
- RFCs that define formal standards have four stages: Proposed Standard (PS), Draft Standard (DS), Standard (STD), and Best Current Practice (BCP)

Internet Architecture Board (IAB)

- Is a subcommittee of the IETF
- Serves as an advisory body to the Internet Society (ISOC)
- Is composed of independent researchers and professionals who have a technical interest in the well-being of the Internet
- Provides oversight for the following:
  - Architecture for Internet protocols and procedures
  - Processes used to create standards
  - Editorial and publication procedures for RFCs
  - Confirmation of IETF chair and technical area directors

Institute of Electrical and Electronics Engineers (IEEE)

- Is an international nonprofit organization that focuses on developing and distributing standards that relate to electricity and electronics
- Has the largest number of members of any technical professional organization in the world
- Supports 39 societies that focus activities on specific technical areas, including magnetics, photonics, and computers
- Provides training and educational opportunities covering a wide number of engineering topics
- Standards are managed by the IEEE Standards Association (IEEE-SA)

Common IEEE 802 Standard Working Groups

Working Group	Name
802.1	Higher Layer LAN Protocols
802.3	Ethernet
802.11	Wireless LAN (802.11a, 802.11b, 802.11g, 802.11n, 802.11ad, etc.)
802.15	Wireless Personal Area Network (WPAN)
802.16	Broadband Wireless Access (WiMAX)
802.18	Radio Regulatory TAG
802.19	Wireless Coexistence
802.20	Mobile Broadband Wireless Access

International Telecommunication Union Telecommunication Sector (ITU-T)

- Is a United Nations agency responsible for managing and promoting information and technology issues
- Performs all ITU standards work and is responsible for ensuring the efficient and effective production of standards covering all fields of telecommunications for all nations
- Divides its recommendations into 26 separate series, each bearing a unique letter of the alphabet
  - For example, switching and signaling recommendations are in the Q series

ITU-T Information Security Recommendations

ITU-T Recommendation	Description
X.800 – X.849: Security	Recommendations in this series address security issues as they relate to different networking layers
X.1000 – X.1099: Information and network security	General network security
X.1100 – X.1199: Secure applications and services	Ensuring that applications and services are developed and deployed in a secure manner

ITU-T Information Security Recommendations (cont.)

ITU-T Recommendation	Description
X.1200 – X.1299: Cyberspace security	Overall cybersecurity, identity management, and countering spam
X.1300 – X.1399: Secure applications and services	Different from X.1100 – X.1199, this series focuses on emergency communications and sensor network security
X.1500 – X.1599: Cybersecurity information exchange	Focused on exchanging information between actors in a secure manner
X.1600 – X.1699: Cloud computing security	Security topics specifically related to cloud environments

American National Standards Institute (ANSI)

- Strives to ensure the safety and health of consumers and the protection of the environment
- Oversees the creation, publication, and management of many standards and guidelines that directly affect businesses in nearly every sector
- Is composed of government agencies, organizations, educational institutions, and individuals
- Produces standards that affect nearly all aspects of IT but primarily software development and computer system operation

ETSI Cyber Security Technical Committee (TC CYBER)

- Develops standards for information and communications technologies (ICT) that are commonly adopted by member countries in the European Union (EU)
- Standards cover both wired and various wireless communication technologies
- Cyber Security Technical Committee, called TC CYBER, centralizes all cybersecurity standards within ETSI committees
- Standards focus on security issues related to the Internet and the business communications it transports

ISO 17799 (Withdrawn)

- A former international security standard that has been withdrawn
- Is a comprehensive set of controls that represent best practices in information systems
  - The ISO 17799 code of practice
  - The BS 17799-2 specification for an information security management system
- Identifies security controls needed for information systems in business environments
- Enables potential customers to evaluate organizations on their efforts toward securing data

ISO 17799 (Withdrawn) (cont.)

The ISO divides the standard into 10 major sections:

- Security Policy
- Security Organization
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- System Development and Maintenance
- Business Continuity Management
- Compliance

ISO/IEC 27002

- Supersedes ISO 17799
- Directs its recommendations to management and security personnel responsible for information security management systems
- Expands on its predecessor by adding two new sections and reorganizing several others

ISO/IEC 27002 (cont.)

New standard has 12 major sections:

- Risk Assessment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Payment Card Industry Data Security Standard (PCI DSS)

- Is an international standard for handling transactions involving payment cards
- Payment Card Industry Security Standards Council (PCI SSC) developed, publishes, and maintains the standard
- Formed by some of the largest payment card vendors who created PCI DSS to protect payment card users from fraud and to preempt legislative requirements on the industry
- Requires layers of controls to protect all payment card-related information as it is processed, transmitted, and stored
- Applies to all organizations that participate in any of the processes surrounding payment card processing

Summary

- International information security standards and their impact on IT infrastructures
- ISO 17799
- ISO/IEC 27002
- Payment Card Industry Data Security Standard (PCI DSS) requirements