Information Security

Course Code: CSC432
Credit Hours: 3(3, 0)
Lecture: 1-2

Dr. Tehsin Kanwal
Assistant Professor

Information Security

This course introduces the concepts and applications of information security. Topics include:

- Information Security Overview;
- Threats & Attacks; Legal & Professional Issues;
- Authentication Models;
- Access Control
- Attack prevention tools and techniques
- Auditing, testing, and monitoring
- Information Security Management & Risk Management
- Information Security Standards, Certifications, and laws

Text and Reference Books Text Book:

1. Principles of Information Security, 6th edition by M. Whitman and H. Mattord
2. Computer Security: Principles and Practice, 3rd edition by William Stallings
3. *Introduction to Computer Security, Goodrich, M., & Tamassia, R., Pearson, 2021*
4. Information Security Policies, Procedures, and Standards by Douglas J. Landoll , O'Reilly , ISBN: 9781315355474
5. CISSP Official Study Guide 7 Edition, by James Michael Stewart, Mike Chapple, and Darril Gibson. PDF available on Moodle. Wiley, ISBN: 978-1-119-04271-6
6. Computer Security, 3rd edition by Dieter Gollmann
7. Computer Security Fundamentals, 3rd edition by William Easttom

What is Information Security

- Information security, is a set of tools and practices that you can use to protect your digital and analog information.
- InfoSec covers a range of IT domains, including infrastructure and network security, auditing, and testing.
- It uses tools like authentication and permissions to restrict unauthorized users from accessing private information. These measures help you prevent harms related to information theft, modification, or loss.

Types of Information Security

- The main objectives of InfoSec are typically related to ensuring confidentiality, integrity, and availability of company information. it involves the implementation of various types of security.
  - Application security.
    - Application security is the use of software, hardware, and procedural methods to protect applications from external threats.
  - Infrastructure security.
    - Infrastructure Security refers to technology assets, including computers, networking systems and cloud resources — both hardware and software.

Types of Information Security

- Database Security
  - Database security is the protection of the database against intentional and unintentional threats that may be computer-based or non-computer-based.
- Data Security
  - Confidentiality and Privacy of Communications
    - Secure system ensures the confidentiality of data, This means that it allows individuals to see only the data they are supposed to see, secure storage of sensitive data.
    - The spread of confidential personal information such as health, employment, and credit records
  - Authentication
    - System verifies a user's identity (proof of identity), an authentication token
  - Authorization
    - An authenticated user goes through the second layer of security, authorization. Authorization is the process through which system obtains information about the authenticated user, including which data the user may access.

Types of Information Security

- Mobile Security
  - Mobile devices-important part in network Smartphones, Tablets, Memory sticks
    - Device Security
    - Traffic Security
    - Barrier Security

Introduction

- Information security: a "well-informed sense of assurance that the information risks and controls are in balance." — Jim Anderson, Inovant (2002)
- Security professionals must review the origins of this field to understand its impact on our understanding of information security today

The History of Information Security

- Began immediately following development first mainframes
  - Developed for code-breaking computations
  - During World War II
    - Multiple levels of security were implemented
- Physical controls
- Rudimentary
  - Defending against physical theft, espionage, and sabotage

The 1960s

- Original communication by mailing tapes
- Advanced Research Project Agency (ARPA)
  - Examined feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception
- Plan
  - Link computers
  - Resource sharing
  - Link 17 Computer Research Centers
  - Cost 3.4M
- ARPANET is predecessor to the Internet

The 1970s and 80s

- ARPANET grew in popularity
- Potential for misuse grew
- Fundamental problems with ARPANET security
  - Individual remote sites were not secure from unauthorized users
  - Vulnerability of password structure and formats
  - No safety procedures for dial-up connections to ARPANET
  - Non-existent user identification and authorization to system

The 1970s and 80s (cont'd.)

- Rand Report R-609
  - Paper that started the study of computer security
  - Information Security as we know it began
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization

MULTICS

- Early focus of computer security research
  - System called Multiplexed Information and Computing Service (MULTICS)
- First operating system created with security as its primary goal
- Mainframe, time-sharing OS developed in mid-1960s
  - GE, Bell Labs, and MIX
- Several MULTICS key players created UNIX
- Late 1970s
  - Microprocessor expanded computing capabilities
  - Mainframe presence reduced
  - Expanded security threats

The 1990s

- Networks of computers became more common
- Need to interconnect networks grew
- Internet became first manifestation of a global network of networks
- **Initially based on de facto standards**
- In early Internet deployments, security was treated as a low priority

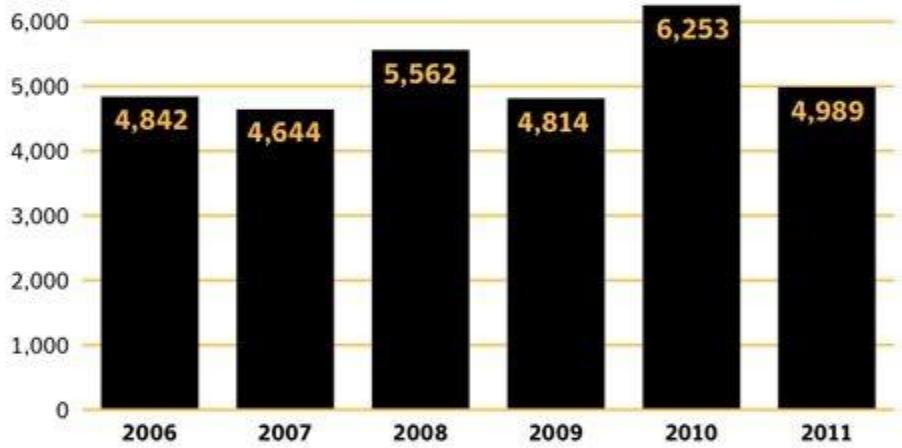
2000 to Present

- Millions of computer networks communicate
- Many of the communication unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected
- Growing threat of cyber attacks has increased the need for improved security

Vulnerabilities

Figure D.1

Total Vulnerabilities Identified, 2006-2011



Source: Symantec.cloud

What is Security?

"the quality or state of being secure—to be free from danger."
In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse
- **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations
- **Operations security**, to protect the details of a particular operation or series of activities
- **Communications security**, to protect communications media, technology, and content
- **Network security**, to protect networking components, connections, and contents
- **Information security**, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

What is Security? (cont'd.)

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle
  - Was standard based on confidentiality, integrity, and availability
  - Now expanded into list of critical characteristics of information

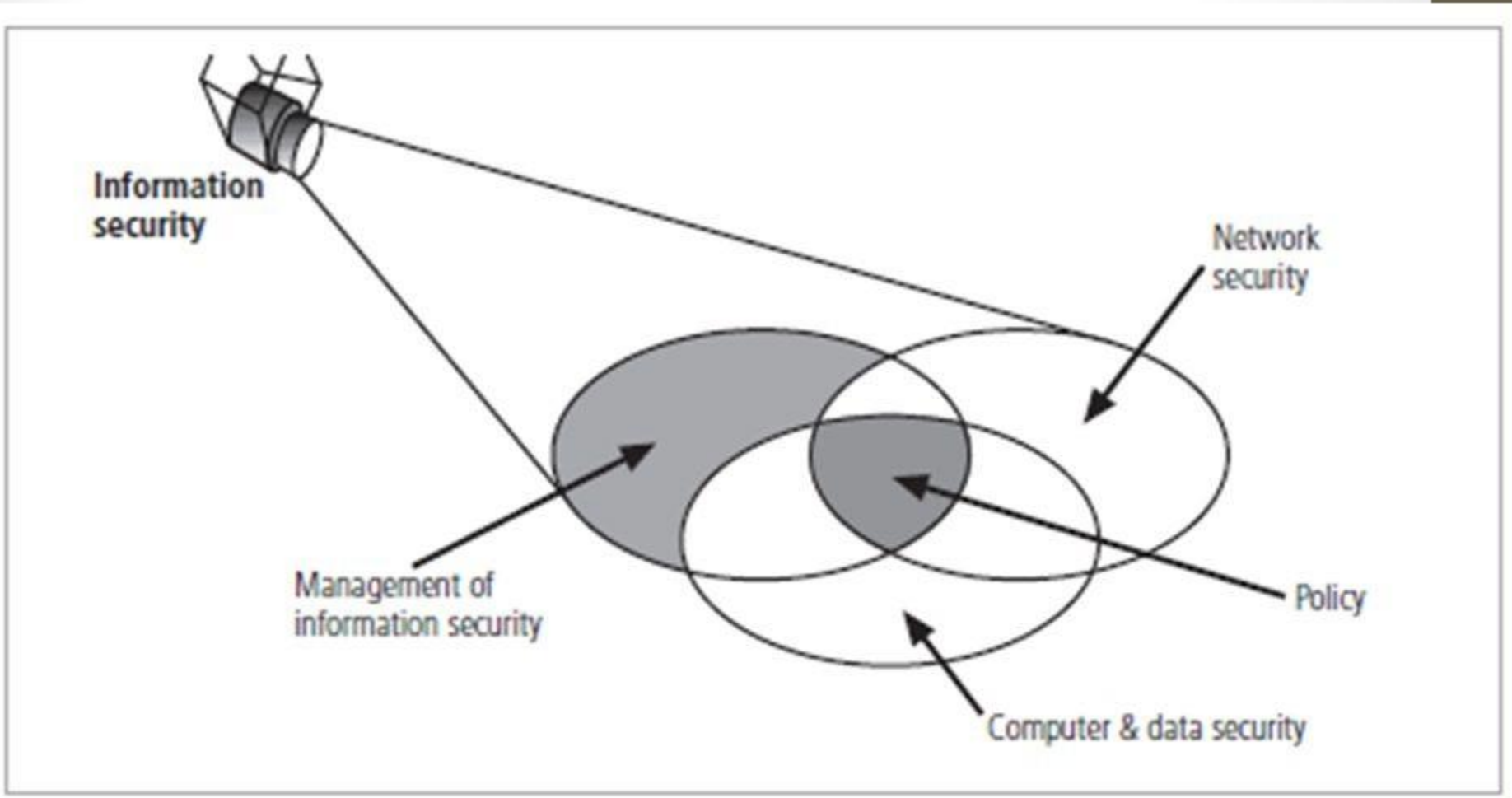


Figure 1-3 Components of Information Security

Key Information Security Concepts

- Access
- Asset
- Attack
- Control, Safeguard, or Countermeasure
- Exploit
- Exposure
- Loss
- Protection Profile or Security Posture
- Risk
- Subjects and Objects
- Threat
- Threat Agent
- Vulnerability

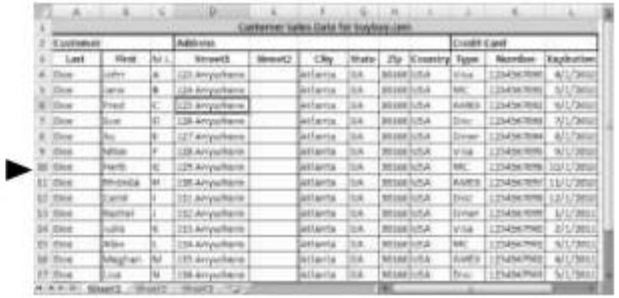
Threat: Theft
Threat agent: Ima Hacker

Vulnerability: Buffer overflow in online database Web interface

Exploit: Script from MadHackz Web site

Attack: Ima Hacker downloads an exploit from MadHackz web site and then accesses buybay's Web site. Ima then applies the script which runs and compromises buybay's security controls and steals customer data. These actions cause buybay to experience a **loss.**

Asset: buybay's customer database



Key Information Security Concepts (cont'd.)

- Computer can be subject of an attack
- Computer can be the object of an attack
  - When the subject of an attack
    - Computer is used as an active tool to conduct attack
  - When the object of an attack
    - Computer is the entity being attacked

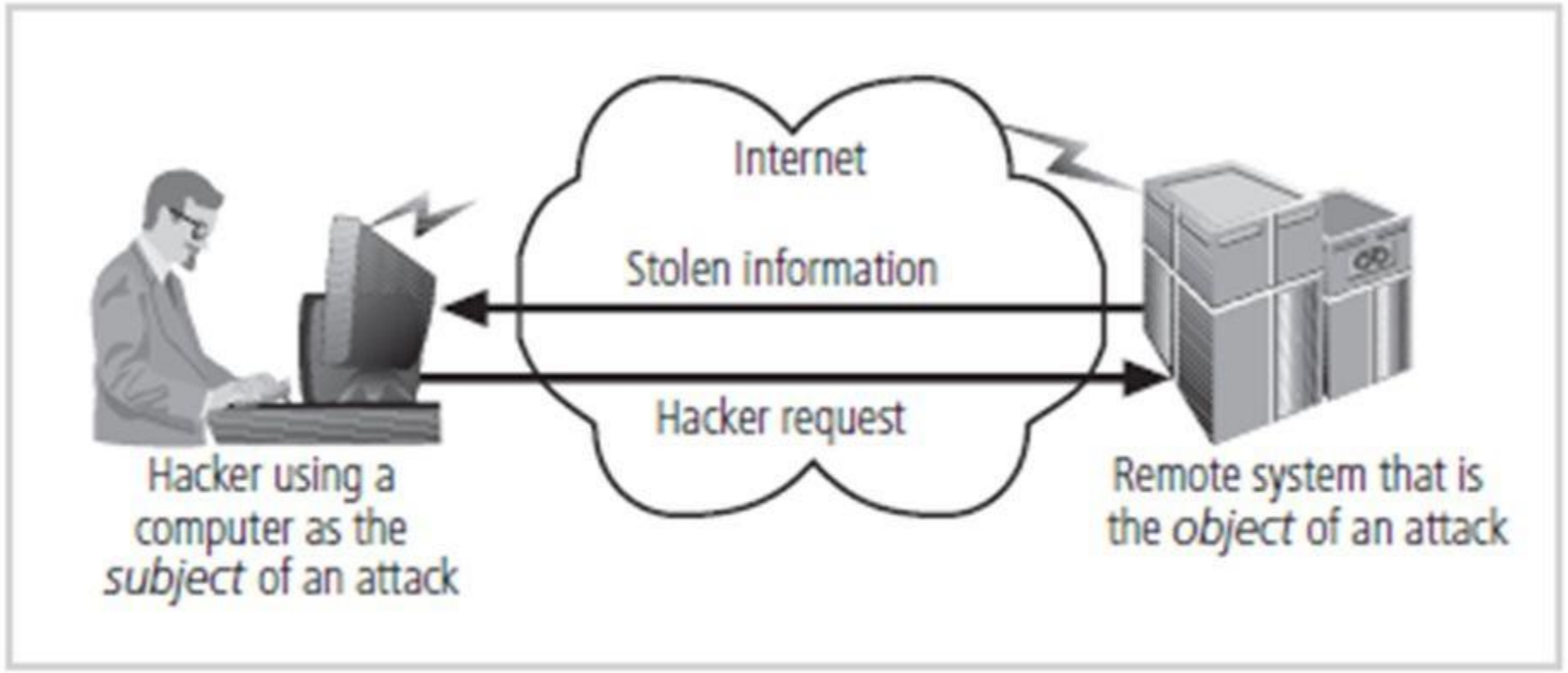


Figure 1-5 Computer as the Subject and Object of an Attack

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility
  - Possession

CNSS Security Model

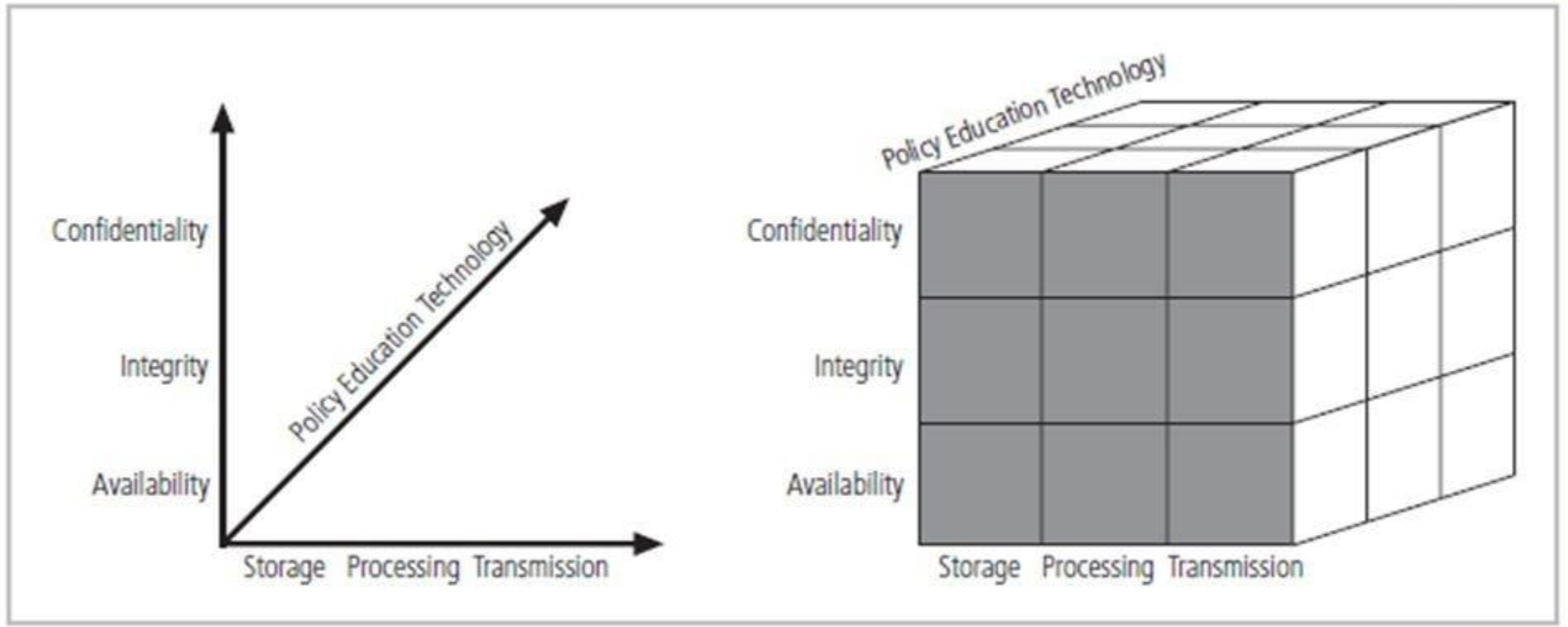


Figure 1-6 The McCumber Cube

McCumber cube

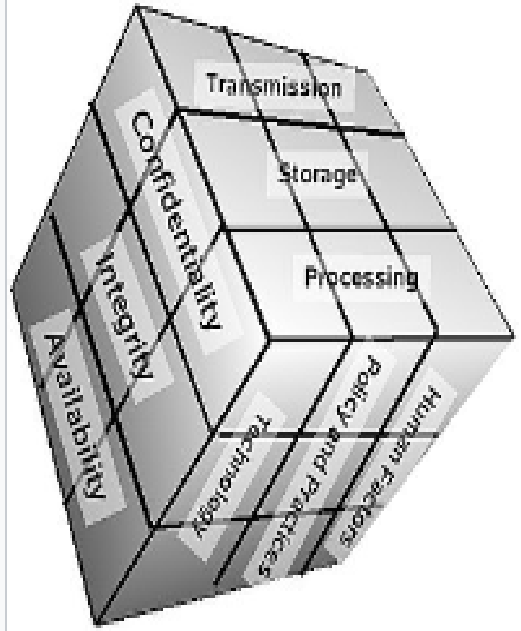
Add languages

Article Talk Read Edit View history

From Wikipedia, the free encyclopedia

In 1991, John McCumber created a model framework for establishing and evaluating information security (information assurance) programs, now known as **The McCumber Cube**. This security model is depicted as a three-dimensional Rubik's Cube-like grid.

The concept of this model is that, in developing information assurance systems, organizations must consider the interconnectedness of all the different factors that impact them. To devise a robust information assurance program, one must consider not only the security goals of the program (see below), but also how these goals relate specifically to the various states in which information can reside in a system and the full range of available security safeguards that must be considered in the design. The McCumber model helps one to remember to consider all important design aspects without becoming too focused on any one in particular (i.e., relying exclusively on technical controls at the expense of requisite policies and end-user training).



The McCumber Cube

Dimensions and attributes [edit]

Desired goals [edit]

- Confidentiality: assurance that sensitive information is not intentionally or accidentally disclosed to unauthorized individuals.
- Integrity: assurance that information is not intentionally or accidentally modified in such a way as to call into question its reliability.
- Availability: ensuring that authorized individuals have both timely and reliable access to data and other resources when needed.

Information states [edit]

- Storage: **Data at rest (DAR)** in an information system, such as that stored in memory or on a magnetic tape or disk.
- Transmission: transferring data between information systems - also known as **data in transit (DIT)**.
- Processing: performing operations on data in order to achieve a desired objective.

Safeguards [edit]

- Policy and practices: administrative controls, such as management directives, that provide a foundation for how information assurance is to be implemented within an organization. (examples: acceptable use policies or incident response procedures) - also referred to as **operations**.
- Human factors: ensuring that the users of information systems are aware of their roles and responsibilities regarding the protection of information systems and are capable of following standards. (example: end-user training on avoiding computer virus infections or recognizing social engineering tactics) - also referred to as **personnel**
- **Technology**: software and hardware-based solutions designed to protect information systems (examples: anti-virus, firewalls, intrusion detection systems, etc.)

Motivation [edit]

Per John McCumber's website, the idea is to push back the advance of security as an art and support it with a structured methodology that functions independent of technology evolution. The basis of this methodology is the inter-relationship among confidentiality, integrity and availability with storage, transmission and processing while applying the policy, procedures, human side and technology.

Components of an Information System

- Information system (IS) is entire set of components necessary to use information as a resource in the organization
  - Software
  - Hardware
  - Data
  - People
  - Procedures
  - Networks

Balancing Information Security and Access

- Impossible to obtain perfect security
- Process, not an absolute
- Security should be considered balance between protection and availability
- Must allow reasonable access, yet protect against threats

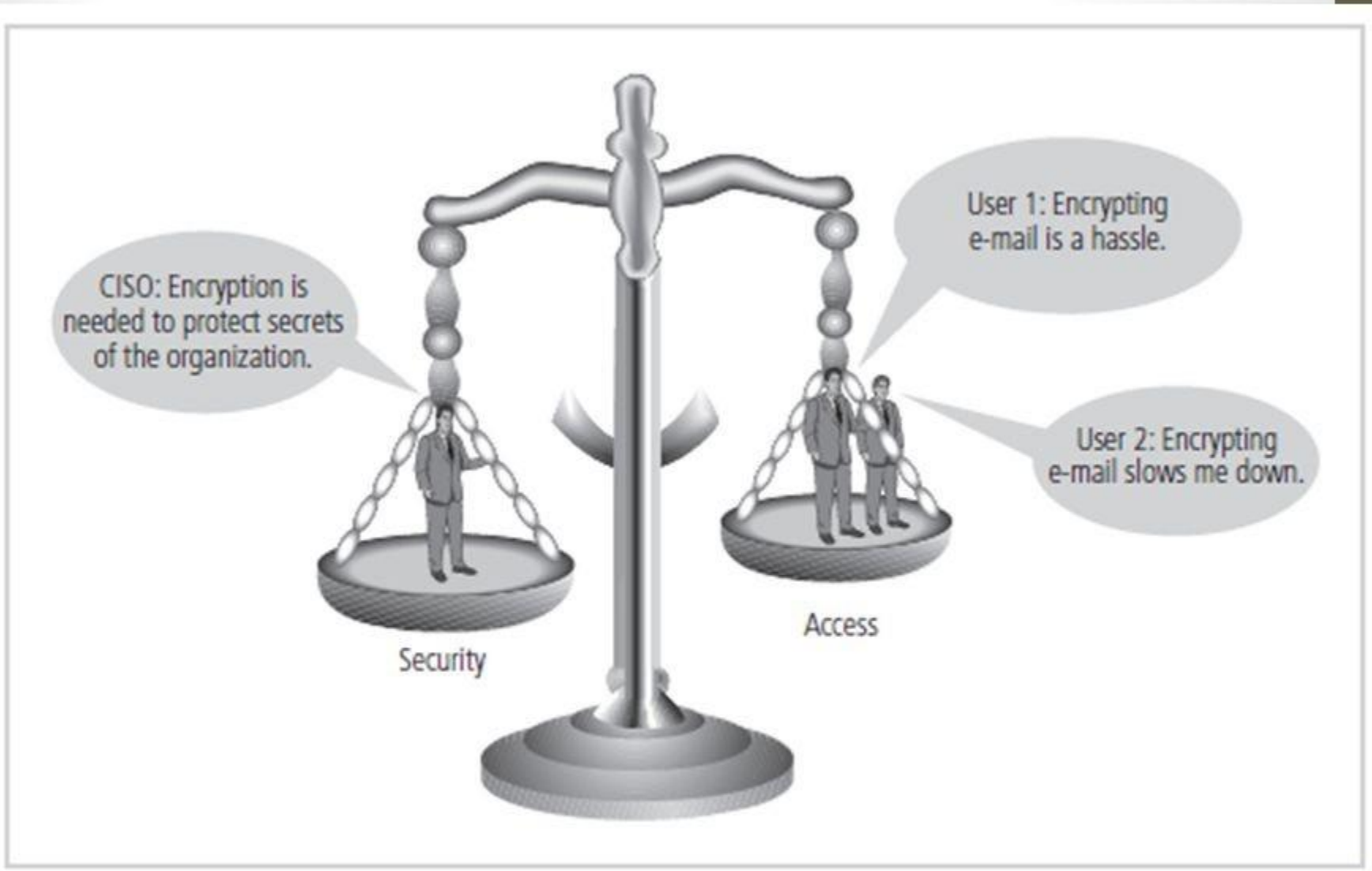


Figure 1-8 Balancing Information Security and Access

Approaches to Information Security Implementation: Bottom-Up Approach

- Grassroots effort -systems administrators drive
- Key advantage: technical expertise of individual administrators
- Seldom works
- Lacks number of critical features:
  - Participant support
  - Organizational staying power

Approaches to Information Security Implementation: Top-Down Approach

- Initiated by upper management
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- Most successful
- Involves formal development strategy
- Systems development life cycle

Information Security Project Team

- A number of individuals who are experienced in one or more facets of required technical and nontechnical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Data Responsibilities

- Data owner: responsible for the security and use of a particular set of information
- Data custodian: responsible for storage, maintenance, and protection of information
- Data users: end users who work with information to perform their daily jobs supporting the mission of the organization

Information Security: Is it an Art or a Science?

- Implementation of information security often described as combination of art and science
- "Security artisan" idea: based on the way individuals perceive systems technologists since computers became commonplace

Security as Art

- No hard and fast rules nor many universally accepted complete solutions
- No manual for implementing security through entire system

Security as Science

- Dealing with technology designed to operate at high levels of performance
- Specific conditions cause virtually all actions that occur in computer systems
- Nearly every fault, security hole, and systems malfunction are a result of interaction of specific hardware and software
- If developers had sufficient time, they could resolve and eliminate faults

Security as a Social Science

- Social science examines the behaviour of individuals interacting with systems
- Security begins and ends with the people that interact with the system
- Security administrators can greatly reduce levels of risk caused by end users, and create more acceptable and supportable security profiles

References

1. *Principles of Information Security, Michael E., Whitman & Mattord, H. J., Cengage Learning, 2017.*
2. *https://www.wikipedia.org/*