Applications and Systems Development

Ed Crowley CISSP
'05

Topics

- Terms
- System Development Life Cycle
- Software Process Capability Maturity Model
- Object Orientated Systems
- Database systems
  - Security issues
  - Data Warehousing
  - Data Mining
  - Data Dictionaries
- Application Control

Certification and Accreditation

Certification

- The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular system's design and implementation meet a set of specified security requirements.

Accreditation

- The formal authorization by the accrediting (management) official for system operation and an explicit acceptance of risk.
  - Usually supported by a system review, including management, operational, and technical controls.

Accountability, Reference Monitor

Accountability

- Means of linking individuals to their interaction with an IT (information technology) product, thereby supporting identification of and recovery from unexpected or unavoidable failures of the control objectives.
- The quality or state that enables actions on a ADP (automated data processing) system to be traced to individuals who may then be held responsible.
  - Actions may include violations and attempted violations of the security policy, as well as allowed actions.

Reference Monitor

- A piece of software that mediates all accesses to objects by subjects.
  - When some process makes an OS call, the reference monitor halts the process and figures out whether the call should be allowed or forbidden.
  - An access control/mediation concept that refers to an abstract machine that mediates all accesses to objects by subjects

Applications And Systems Development Security

- Refers to controls included within systems and applications software and the steps used in their development.
  - Applications refer to agents, applets, software, database, data warehouses, and knowledge-based systems.
  - The applications may be used in distributed or centralized environments.

SDLC Goals

- Produce quality software
  - Within allocated budget and time.
- Several models:
  - Waterfall Model
  - Spiral Model
  - Information Security and the Life Cycle Model

Waterfall Model

- Software development managed by allowing developers to going back only one stage to rework.
- Verification doing the job right
  - During development phase
- Validation doing the right job
  - At end of development phase

Spiral Model

- Meta Model incorporating a number of other software models.
- Angular dimension represents the progress made in completing the phases
- Radial dimension represents cumulative project cost.
- Each spiral cycle involves the same series of steps for each part of the project.

Four QuadrantsRequirements, Objective, Planning, Risk Analysis

- Lower Left Quadrant
  - Focuses on developing plans that will be reviewed in the upper quadrants.
- Upper left
  - Defines the objectives of the part of the project being addressed, alternative means of accomplishing this part, and constraints associated with these alternatives.
- Next quadrant
  - Involves assessing the alternatives in regard to the project objectives and constraints.
- Lower right quadrant
  - Depicts the final developmental phase for each part of the product.

Information Security and the Life Cycle model

- Information security controls:
  - Conception
  - Development
  - Implementation
  - Testing and
  - Maintenance
- Should be conducted concurrently with the system software life cycle phases.
- Testing
  - Personnel separate from the programmers should conduct the testing

Risk Management and Assessments

- Should start at the beginning of a project and continue throughout the lifetime of the project.
- Without proper design, more effort will have to take place in the implementation, testing, and maintenance phases.

Software Maintenance Phase and the Change Control Process

- Three sub phases
  - Request control
  - Change control
  - Release control

Request Control

- Establishes the request's priorities
- Estimates cost of requested changes
- Determines the interface that is presented to the user.

Configuration Control: Tracking and Issuing New Versions

- Needs to be in place at the beginning of a project.
- Must be enforced through each phase.
- Two Goals:
  1. Changes must not affect the security level of the system or its capability to enforce the security policy.
  2. Changes must be documented
     - Changes must be authorized, tested, and recorded.

Software Capability Maturity Model (CMM)

- Process defined by Carnegie Mellon's Software Engineering Institute.
- "A process is a set of activities, methods, practices and transformation that people use to develop and maintain systems and associated products.

Five CMM Maturity Levels

- Initiating – Competent people and heroics
- Repeatable – Project management processes
- Defined – Engineering processes and organizational support (Requires ISO 9001)
- Managed – Product and process improvement
- Optimizing – Continuous process improvement

Object Oriented Systems

- In theory, objects provide modularity, reusability, and more granular control.
- Group of independent objects can be requested to perform certain operation or exhibit specific behaviors.
- Objects have state, behavior, and identity.
- Objects can encapsulated data
  - Encapsulation is the process of compartmentalizing the elements of an abstraction that constitute its structure and behavior a.k.a. data hiding.
- When an action takes place on an object, it is referred to as a method.

OO

- By reusing tested and reliable objects, applications can be developed in less time and at less cost.
- Objects are members, or instances, of classes.
  - Classes dictate the objects data types, structure, and acceptable actions.

CORBA

- Common Object Request Broker Architecture
  - Developed by the Object Management Group (OMG).
- Provides a standardized way for objects within different applications, platforms, and environments to communicate.
  - Provides standards for object's interfaces.

Common Object Model (COM)

- Provides an architecture for components to interact on a local system.
- Distributed COM (DCOM) uses the same interfaces as COM but enables components to interact of a distributed or networked environment.

Artificial Intelligence Systems

Two types:

- Expert systems
- Neural networks

Expert Systems

- Accomplishes reasoning by building a knowledge base of the domain to be addressed in the form of rules and an inference mechanism to determine if the rules have been satisfied by the system input.
- Inference engine + knowledge base = expert system

Knowledge Base

- Contains facts and rules concerning the domain of the problem in the form of If – Then statements.

Neural Networks

- Based on the functioning of biological neurons.
- Attempt to mimic a brain by using units that react like neurons.

Database Systems

- General mechanisms for defining, storing, and manipulating data.
- Database types
  - Relational
  - Hierarchical
  - Mesh
  - Object Orientated

Database Security Issues

- Views – virtual relation that combines information from other relations.

Aggregation and Inference

- Aggregation
  - The act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity.
- Inference
  - The ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privileges.

Data Warehouse and Data Mining

- Data in a data warehouse is normalized i.e. redundant data is removed.
- Data mining is the process of searching for data correlations in a data warehouse.
- A data dictionary is a database for system developers.

Application Controls

- The goal of application controls is to enforce the organization's security policy and procedures and to maintain the confidentiality, integrity, and availability of the computer based information.

Distributed Systems

- Special security challenge.
- Server provides access to data, holds the databases, provides data to the client, performs backups, and provides security services.
- Agent surrogate program or process performing services in one environment on behalf of a principal in another environment.

Questions?