InfoSec Tutorial: Applications & Development

Tony Kenyon, CEO.

Revision 1.01.
Updated: Jan 5th 2006

Ref: CNXT0005

Applications & System Development

- Terms
  - Verification: does the software meet its specification
  - Validation: fitness of the software for its mission
  - Requirements: a complete validated specification of the required functions, interfaces, & performance for a software product
  - Product Design: complete, verified specification of the overall hw-sw architecture, control structure, and data structure for a product.
  - ”Verification is doing the job right, and validation is doing the right job” [Barry Boem]

Development Models

- Development Models
  - Waterfall Model [1970 W.W.Royce]
  - Modified Waterfall Model [1976 Bary Boem]
    - Added milestones, reverse loops as verification-validation points
  - Spiral Model [Barry Boem 1988]
    - Meta Model, progress verses cost spiral
- Cost Models
  - COCOMO Model [1981 Barry Boem]
  - Function Point Measured Model
  - Software Life Cycle Model
    - Uses Rayleigh curve, Manpower Build Index (MBI), Productivity Factor (PF)

COCOMO Models

- Basic COCOMO [1981 Barry Boem]

  $MM = 2.4 (KDSI)^{1.05}$

  $TDEV = 2.5 (MM)^{0.38}$

  - MM= man months. KDSI=thousands of delivered source code lines. TDEV=development schedule (months)
  - Assumes average project
- Intermediate COCOMO
  - Takes account of hardware constraints staff quality, tools etc.
- Detailed COCOMO

Configuration Management

- Configuration Management as per BS7799 1998
  - Config Item
  - Version
  - Configuration
  - Bilding
  - Build List
  - Software Library

Software Capability Maturity Model (CMM)

- Quality of sw is a direct function of its associated development and maintenence processes.
- Defined by CMU Software Engineeering Institute (SEI)
  - See ”The Capability Maturity Model: Guidelines for Improving the Software Process”, Addison Wesley, 1995.
  - Continuous Improvement Model (based on IDEAL Model)
- Five Levels (IRDMO)
  - 1 Initiating
  - 2 Repeatable
  - 3 Defined
  - 4 Managed
  - 5 Optimizing

Object-Oriented Systems

- Terms
  - Message
  - Method
  - Behavior
  - Class
  - Instance
  - Inheritance
  - Multiple Inheritance
  - Delegation
  - Polymorphism
  - Polyinstantiaton
  - Encapsulation: objects are black boxes accessed through messages

Object Request Architecture (ORA)

- CORBA
- COM
  - Formerly OLE
- J2EE
- .NET

Databases

- Architectures
  - Hierarchical
  - Mesh
  - Object-Oriented
  - Relational
- Relational
  - Security provided via ’views’
- Issues
  - Circumventing security controls
  - Aggregation & Inference

Databases

- Data Wharehouse
  - Subject-oriented integrated normalised database used to support management decision making
  - Takes cleaned up (normalised) data from operational databases
  - Data Scrubbing (periodic maintenence of data to see if it is still valid)
- On-Line Analytical Processing (OLAP)
- Decision Support System (DSS)
- Data Mart
  - Comprises data/relations derived from a data wharehouse
- Data Mining
  - Search for new correlations, relations and meta-data in a data wharehouse
- Data Dictionary
  - A database for system developers (data structures)

Secure Storage

- RAID
- Disk Mirroring: duplicate disk
- Disk Duplexing: duplicate disk controller
- FT System: full detection and auto-correction at the system level

Further Research

- Security Life Cycle Model

Questions?