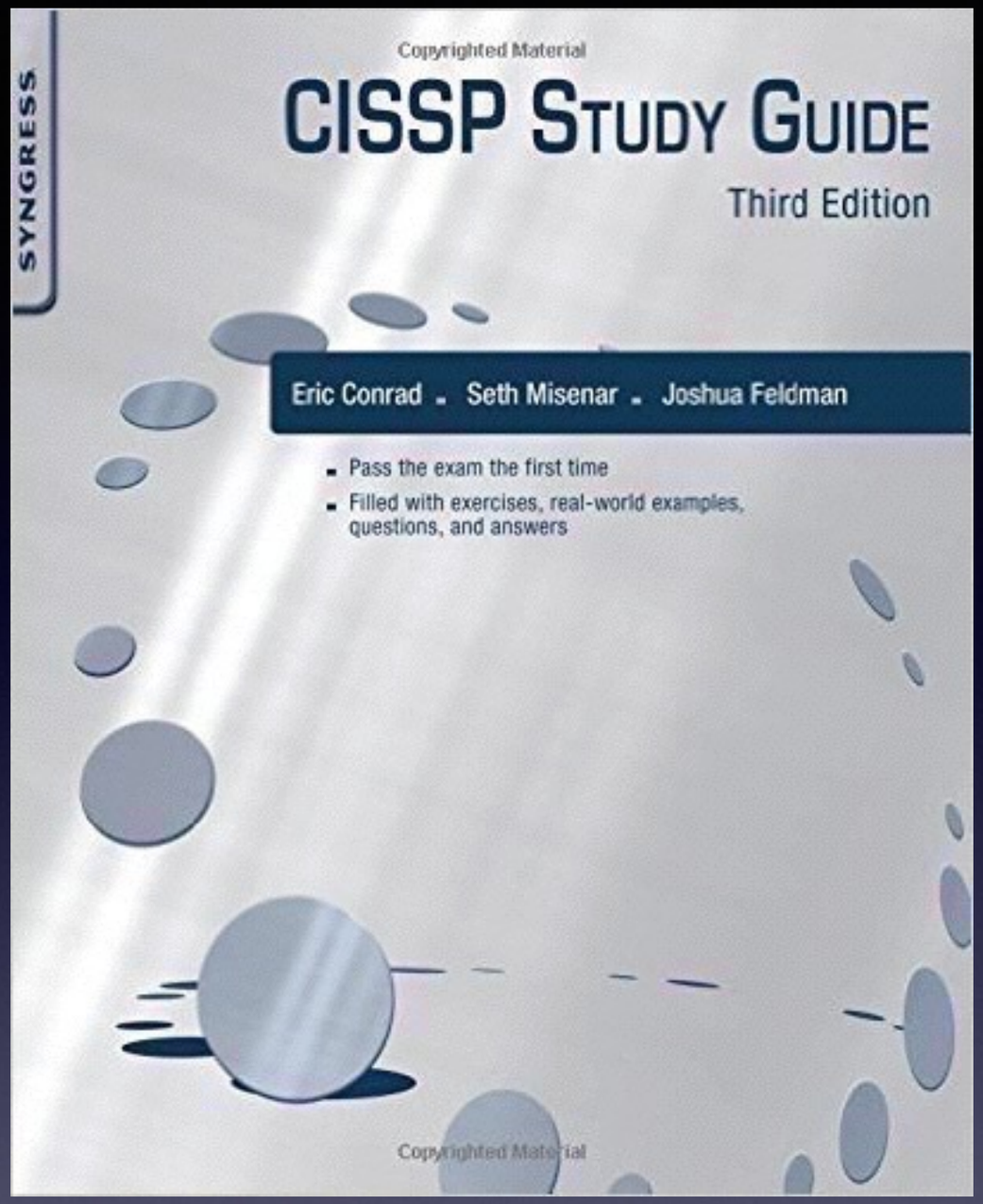
CNIT 125: Information Security Professional (CISSP Preparation)



Ch 9. Software Development Security

Programming Concepts

Machine Code, Source Code, and Assembly Language

- **Machine code**
  - **Binary language built into CPU**
- **Source code**
  - **Human-readable language like C**
- **Assembly Language**
  - **Low-level commands one step above machine language**
  - **Commands like ADD, SUB, PUSH**

Compilers, Interpreters, and Bytecode

- **Compilers translate source code into machine code**
- **Interpreters translate each line of code into machine code on the fly while the program runs**
- **Bytecode is an intermediary form between source code and machine code, ready to be executed in a Java Virtual Machine**

Procedural and Object-Oriented Languages

- **Procedural languages use subroutines, procedures and functions**
  - **Ex: C, FORTRAN**
- **Object-oriented languages define abstract objects**
  - **Have attributes and methods**
  - **Can inherit properties from parent objects**
  - **Ex: C++, Ruby, Python**

Metasploit Source Code

```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::FileDropper

  def initialize(info={})
    super(update_info(info,
      'Name'           => 'ATutor 2.2.1 SQL Injection / Remote Code Execution',
      'Description'    => %q{
        This module exploits a SQL Injection vulnerability and an authentication weakness
```

- **Link Ch 9a**

Fourth-Generation Programming Languages (4GL)

- **Automate creation of code**

- First-generation language: machine code
- Second-generation language: assembly
- Third-generation language: COBOL, C, Basic
- Fourth-generation language: ColdFusion, Progress 4GL, Oracle Reports

Computer-Aided Software Engineering (CASE)

- **Programs assist in creation and maintenance of other programs**
- **Three types**
  - **Tools: support one task**
  - **Workbenches: Integrate several tools**
  - **Environments: Support entire process**
- **4GL, object-oriented languages, and GUIs are used as components of CASE**

Top-Down vs. Bottom-Up Programming

- **Top-Down**
  - **Starts with high-level requirements**
  - **Common with procedural languages**
- **Bottom-Up**
  - **Starts with low-level technical implementation details**
  - **Common with object-oriented languages**

Types of Publicly Released Software

- **Closed Source**
  - **Source code is confidential**
- **Open Source**
- **Free Software**
  - **May cost $0, or be open to modify**
- **Freeware: costs $0**
- **Shareware: free trial period**
- **Crippleware: limited free version**

Software Licensing

- **Public domain (free to use)**
- **Proprietary software is copyrighted, and sometimes patented**
- **EULA (End User License Agreement)**
- **Open-source licenses**
  - **GNU Public License (GPL)**
  - **Berkeley Software Distribution (BSD)**
  - **Apache**

Application Development Methods

Waterfall Model

- **From 1969**
- **One-way**
- **No iteration**
- **Unrealistic**

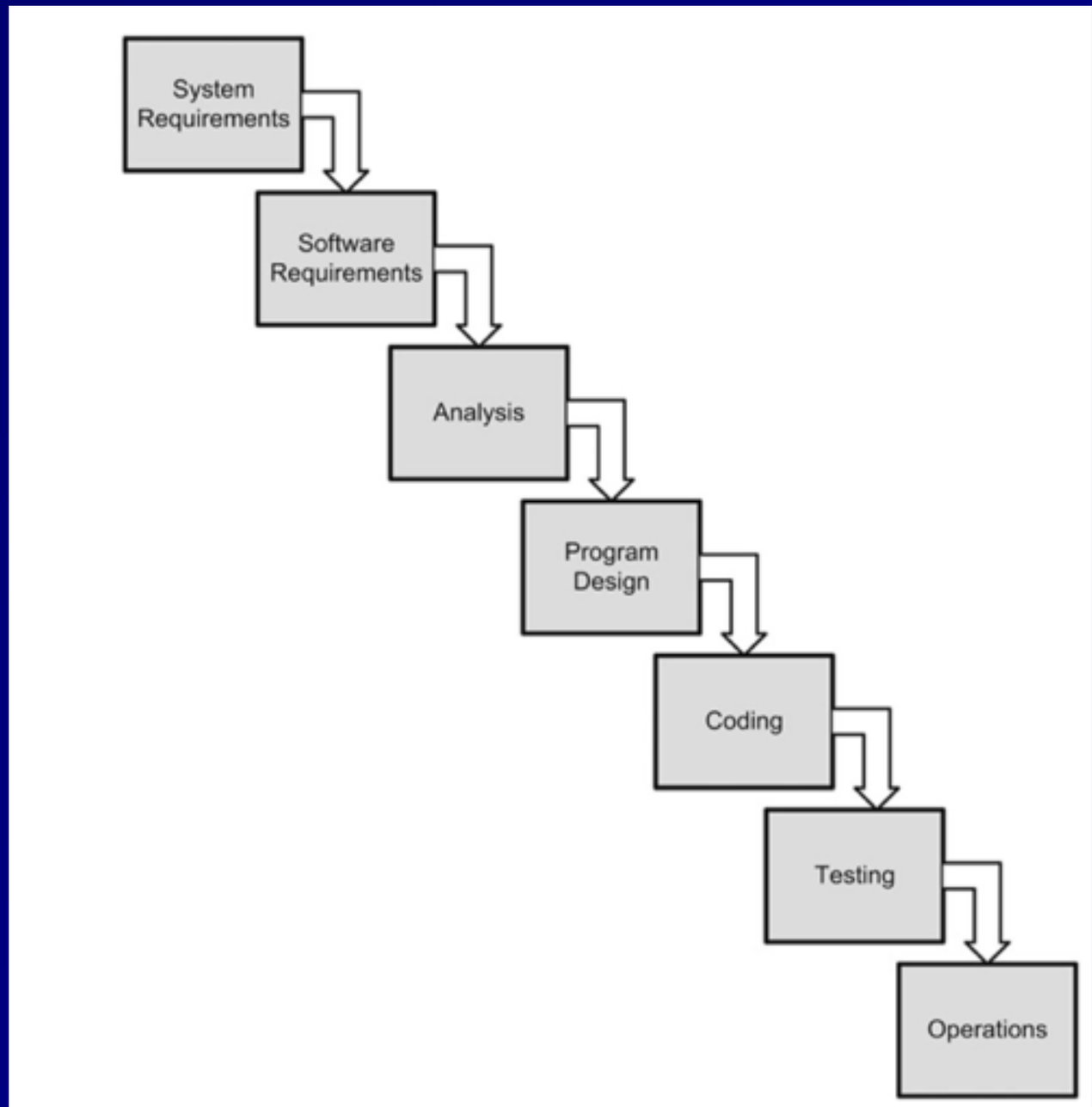


FIGURE 9.1 Unmodified Waterfall Development Model [6]

Modified Waterfall Model

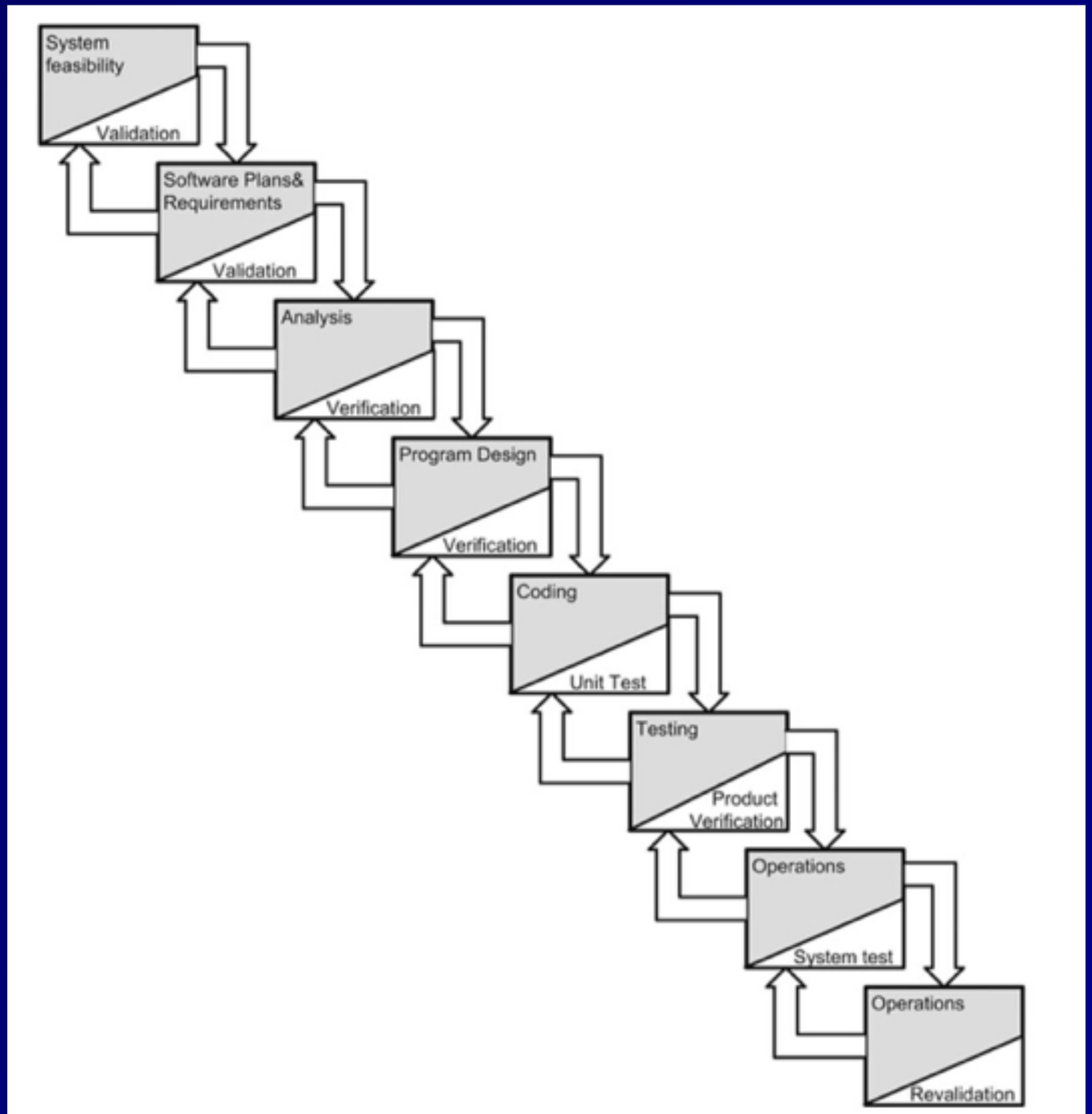


FIGURE 9.2 **Modified Waterfall Development Model [9]**

Sashimi Model

- **Steps overlap**

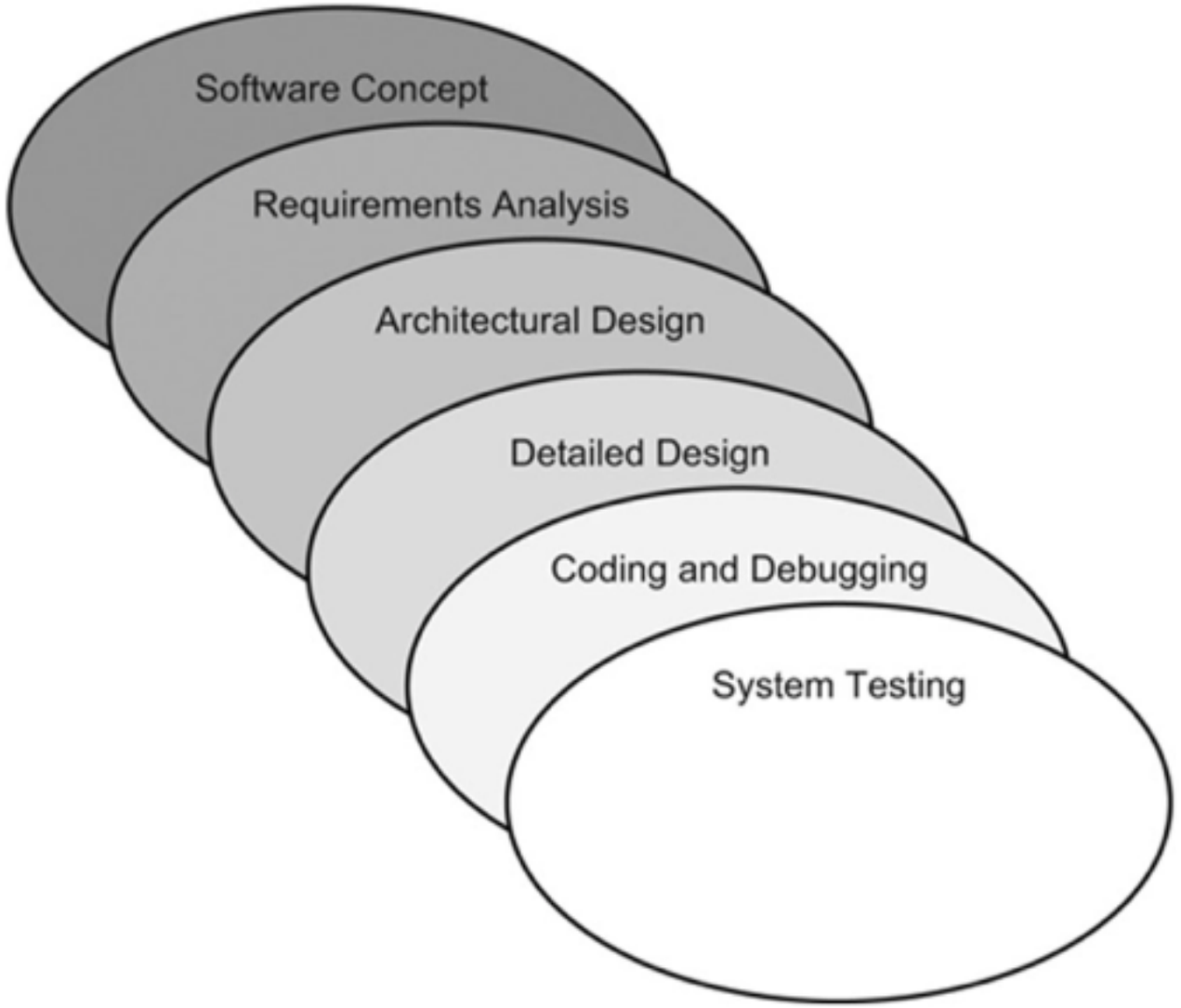


FIGURE 9.3 The Sashimi Model [11]

Agile Software Development

- **Agile methods include Scrum and Extreme Programming (XP)**
- **Agile Manifesto**

"We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan" [12]

Scrum

- **Stop running the relay race**
  - **Doing only one step and handing off the project**
- **Take up rugby**
  - **A team goes the distance as a unit**

Extreme Programming (XP)

- **Pairs of programmers work off a detailed specification**
- **Constant communication with fellow programmers and customers**

- Planning: specifies the desired features, which are called the User Story. They are used to determine the iteration (timeline) and drive the detailed specifications.
- Paired programming: programmers work in teams.
- Forty-hour workweek: the forecasted iterations should be accurate enough to forecast how many hours will be required to complete the project. If programmers must put in additional overtime, the iteration must be flawed.
- Total customer involvement: the customer is always available, and carefully monitors the project.
- Detailed test procedures: they are called Unit Tests.[16]

Spiral

- **Many rounds**
- **Each round is a project; may use waterfall model**
- **Risk analysis performed for each round**

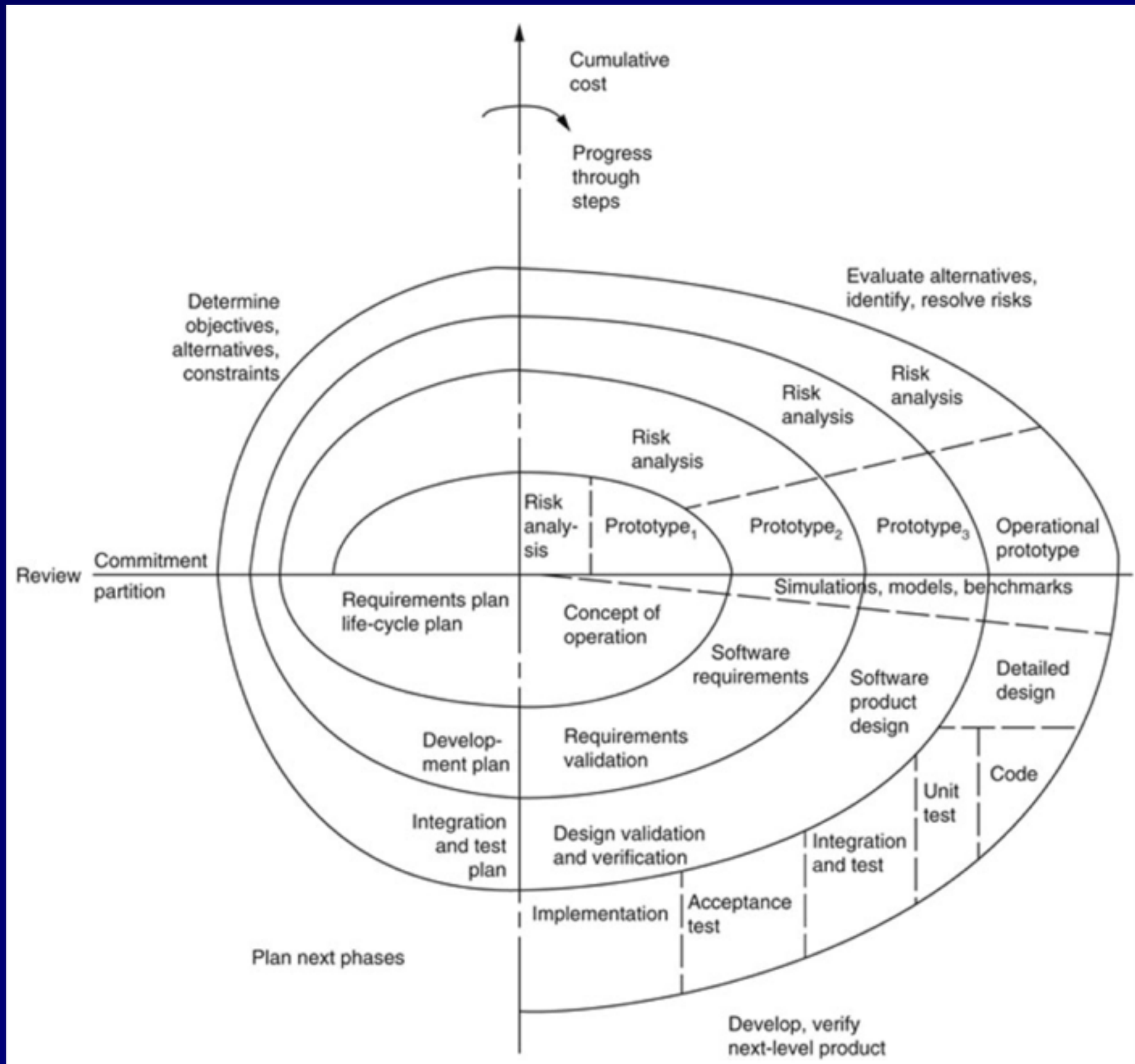


FIGURE 9.4 The Spiral Model [19]

Rapid Application Development (RAD)

- **Goal: quickly meet business needs**
- **Uses prototypes, "dummy" GUIs, and back-end databases**

Prototyping

- **Breaks projects into smaller tasks**
- **Create multiple mockups (prototypes)**
- **Customer sees realistic-looking results long before the final product is completed**

SDLC

- **Systems Development Live Cycle**
- **or Software Development Live Cycle**
- **Security included in every phase**
- **NIST Special Publication 800-14**

SDLC Phases

- **Initiation**
- **Development / Acquisition**
- **Implementation**
- **Operation**
- **Disposal**

- **Security plan should be first step**

SDLC Overview

- **Prepare security plan**
- **Initiation: define need and purpose**
  - **Sensitivity Assessment**
- **Development / Acquisition**
  - **Determine security requirements and incorporate them into specifications**
- **Implementation**
  - **Install controls, security testing, accreditation**

SDLC Overview

- **Operation / Maintenance**
  - **Security operations and administration: backups, training, key management, etc.**
  - **Audits and monitoring**
- **Disposal**
  - **Archiving**
  - **Media sanitization**

Integrated Product Teams

- **A customer-focused group that focuses on the entire lifecycle of a project**
- **More agile than traditional hierarchical teams**

Software Escrow

- **Third party archives source code of proprietary software**
- **Source code is revealed if the product is orphaned**

Code Repository Security

- **Like GitHub**
- **Contents must be protected**
- **Developers shouldn't publish code that contains secrets**

Security of Application Programming Interfaces (APIs)

- **API allows apps to use a service, like Facebook**
- **API exploits abuse the API to compromise security**

OWASP Enterprise Security API Toolkits

- Authentication
- Access control
- Input validation
- Output encoding / escaping
- Cryptography
- Error handling and logging
- Communication security
- HTTP security
- Security configuration [32]

Software Change and Configuration Management

- **Ensures that changes occur in an orderly fashion, and don't harm security**
- **NIST SP 80-128 describes a Configuration Management Plan (CMP)**
  - **Configuration Control Board (CCB)**
  - **Configuration Item Identification**
  - **Configuration Change Control**
  - **Configuration Monitoring**

DevOps

- **Old system had strict separation of duties between developers, quality assurance, and production**
- **DevOps is more agile, with everyone working together in the entire service lifecycle**

Databases

Database

- **Structured collection of data**
- **Databases allow**
  - **Queries (searches)**
  - **Insertions**
  - **Deletions**
- **Database Management Systems (DBMS)**
  - **Controls all access to the database**
  - **Enforces database security**

Database Concepts

- **Database Administrator (DBA)**
- **Query language**
  - **Ex: Structured Query Language (SQL)**
- **Inference attack**
  - **Enumerating low-privilege data to find missing items, which must be high-privilege**
- **Aggregation attack**
  - **Combining many low-privilege records to deduce high-privilege data**

Types of Databases

- **Relational**
- **Hierarchical**
- **Object-oriented**
- **Flat file**
- **Simple text file**

Relational Databases

2. SQL Database Structure

The database named **`sqlol`** contains the two tables shown below.

Table: `users`

Field: `username`	Field: `isadmin`
Herp Derper	1
SlapdeBack LovedeFace	1
Wengdack Slobdegoob	0
Chunk MacRunfast	0
Peter Weiner	0

Table: `ssn`

Field: `name`	Field: `ssn`
Herp Derper	111-11-1111
SlapdeBack LovedeFace	222-22-2222
Wengdack Slobdegoob	333-33-3333
Chunk MacRunfast	444-44-4444
Peter Weiner	555-55-5555

Important Terms

Database -- an object that contains Tables
Table -- an object that contains Fields
Field -- an item of data, such as a name or ssn

Relational Database Terms

- **Tables have rows (records or tuples) and columns (fields or attributes)**
- ***Primary Key* field is guaranteed to be unique, like a SSN**
- ***Foreign key* is a field in another table that matched the primary key**
- ***Join* connects two tables by a matching field**

Integrity

- **Referential Integrity**
  - **Foreign keys match primary keys**
- **Semantic Integrity**
  - **Field values match data type (no letters in numerical fields)**
- **Entity Integrity**
  - **Each tuple has a non-null primary key**

Table 9.3

Database Table Lacking Integrity

SSN	Vacation Time	Sick Time
467-51-9732	7 days	14 days
737-54-2268	3 days	Nexus 6
133-73-1337	16 days	22 days
133-73-1337	15 days	20 days

Database Normalization

- **Removes redundant data**

- First Normal Form (1NF): Divide data into tables.
- Second Normal Form (2NF): Move data that is partially dependent on the primary key to another table. The HR Database (Table 9.2) is an example of 2NF.
- Third normal Form (3NF): Remove data that is not dependent on the primary key. [35]

Database Views

- **Contained user interface**
- **Shows only some data and options**
- **Like a PoS (Point of Sale) device**

Data Dictionary

- **Describes the tables**
- **This is *metadata* -- data about data**
- **Database schema**
  - **Describes the attributes and values of the tables**

Simple Database Schema

Table	Attribute	Type	Format
Employee	SSN	Digits	###-##-####
Employee	Name	String	<30 characters>
Employee	Title	String	<30 characters>
HR	SSN	Digits	###-##-####
HR	Sick Time	Digits	### days
HR	Vacation Time	Digits	### days

Query Languages

- **Two subsets of commands**
  - **Data Definition Language (DDL)**
  - **Data Manipulation Language (DML)**
- **Structured Query Language (SQL) is the most common query language**
- **Many types**
  - **MySQL, ANSI SQL (used by Microsoft), PL/SQL (Procedural Language/SQL, used by Oracle), and more**

Common SQL Commands

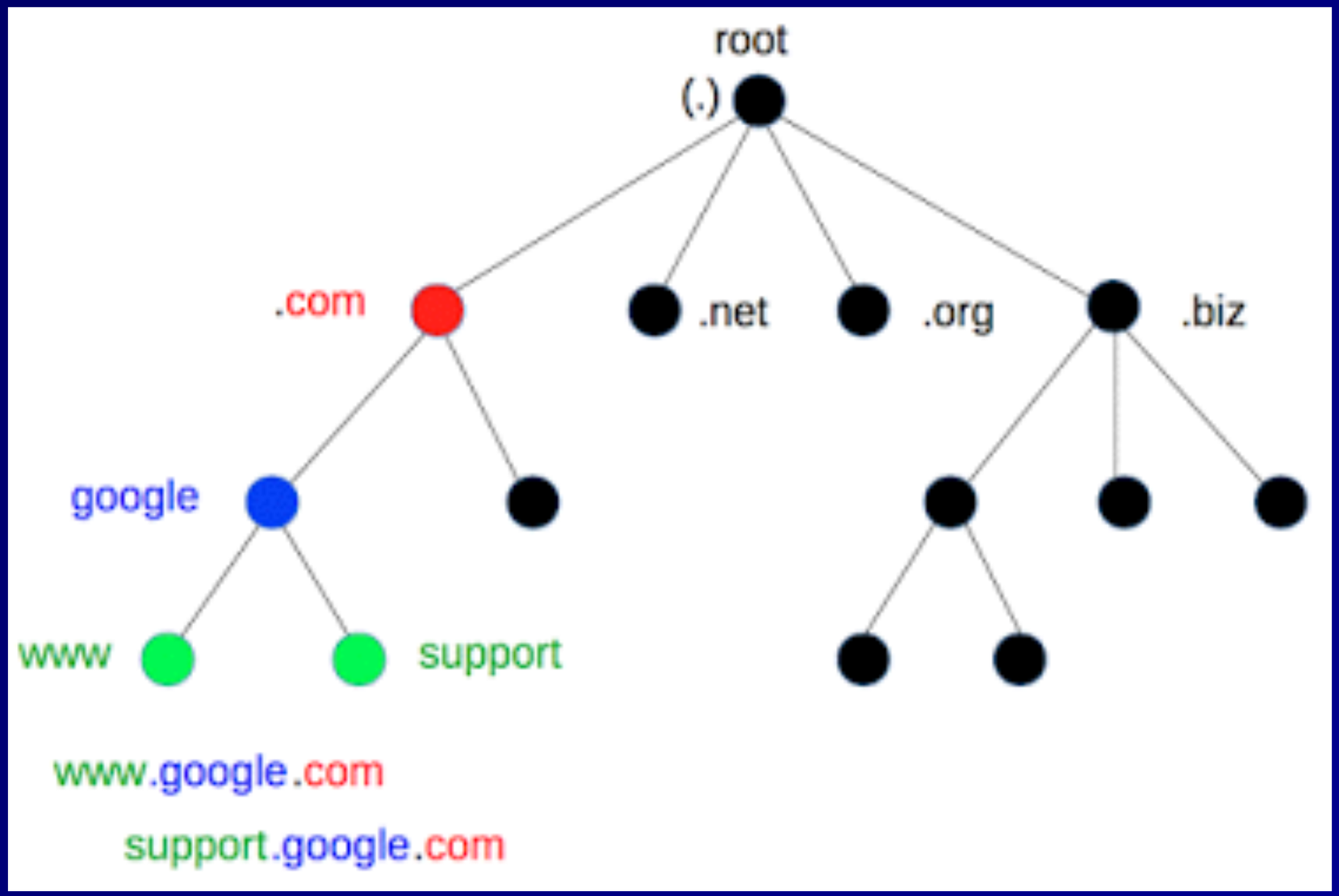
Common SQL commands include:

- CREATE: create a table
- SELECT: select a record
- DELETE: delete a record (or a whole table)
- INSERT: insert a record
- UPDATE: change a record

- **SELECT * FROM Employees WHERE Title = "DETECTIVE"**

Hierarchical Databases

- **A tree, like DNS**



Object-Oriented Databases

- **Combines data and functions in an object-oriented framework**
- **Uses Object Oriented Programming (OOP)**
- **and Object Database Management System (OBMS)**

Database Integrity

- **Mitigate unauthorized data modification**
- **Two users may attempt to change the same record simultaneously**
- **The DBMS attempts to *commit* an update**
- **If the commit is unsuccessful, the DBMS can *rollback* and restore from a *save point***
- ***Database journal* logs all transactions**

Database Replication and Shadowing

- **Highly Available (HA) databases**
  - **Multiple servers**
  - **Multiple copies of tables**
- **Database replication**
  - **Mirrors a live database**
  - **Original and copy are in use, serving clients**
- **Shadow database**
  - **Live backup, not used**

Data Warehousing and Data Mining

- **Data Warehouse**
  - **A large collection of data**
  - **Terabytes (1000 GB)**
  - **Petabytes (1000 TB)**
- **Data Mining**
  - **Searching for patterns**
  - **Ex: finding credit card fraud**

Object-Oriented Design and Programming

Object-Oriented Programming (OOP)

- **A program is a series of connected objects that communicate via messages**
  - **Ex: Java, C++, Smalltalk, Ruby**
- **Objects contain data and *methods***
- **Objects provide *data hiding***
  - **Internal structure not visible from the outside**
  - **Also called *encapsulation***

Object-Oriented Programming Concepts

- **Objects**
- **Methods**
- **Messages**
- **Inheritance**
- **Delegation**
- **Polymorphism**
- **Polyinsstantiation**

Example

- **Addy is an object**
- **It has a *method* of addition**
- **Input message is "1+2"**
- **Output message is "3"**

FIGURE 9.6 The "Addy" Object

Example

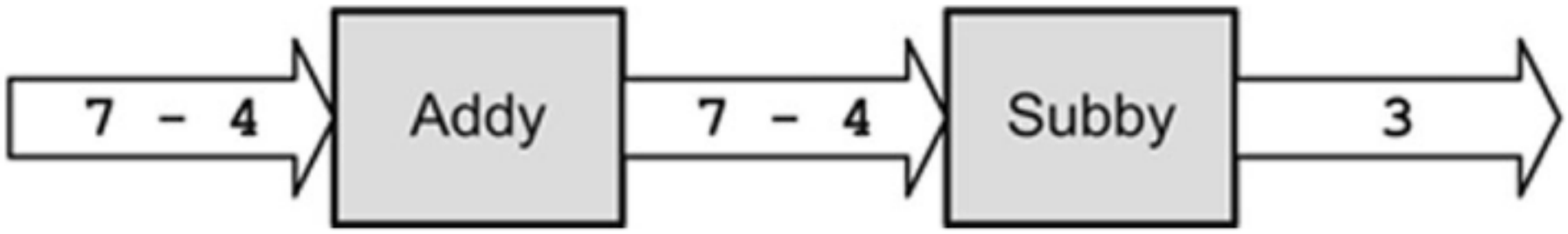


FIGURE 9.7 Delegation

FIGURE 9.8 Polymorphism

Polyinstantiation

- **Multiple records for the same primary key, with different clearance levels**

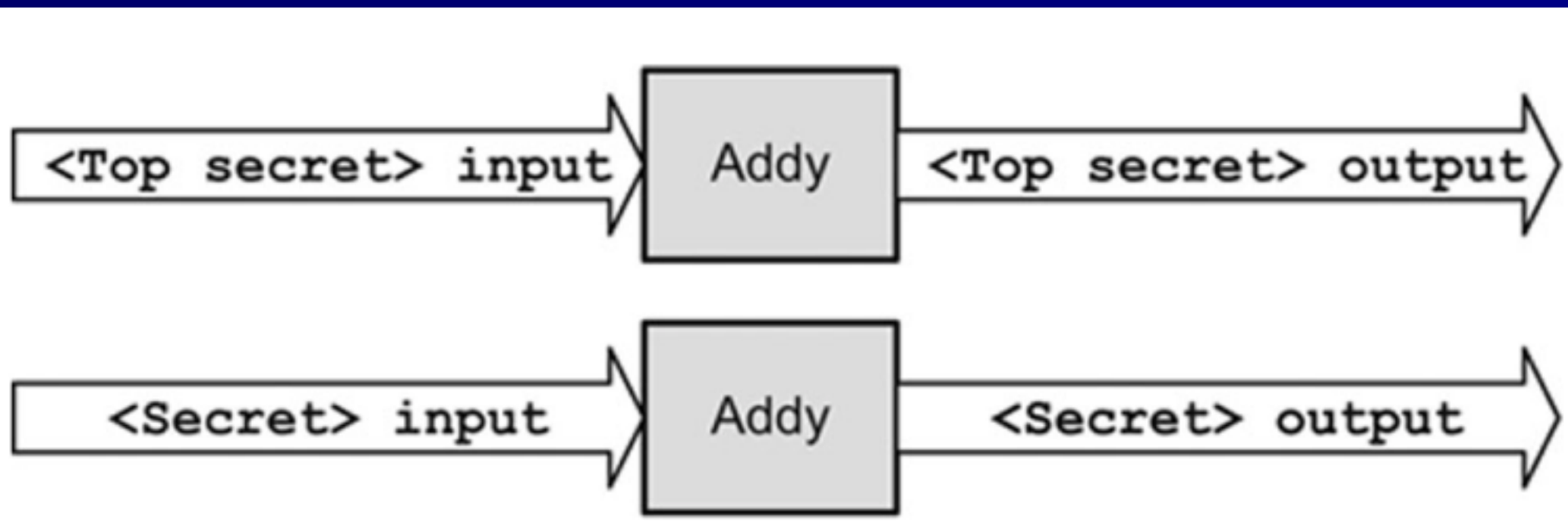


FIGURE 9.9 Polyinstantiation

Object Request Brokers (ORBs)

- **Middleware**
  - **Connect programs to other programs**
  - **Object search engines**
- **Common ORBs**
  - **COM, DCOM, CORBA**

COM and DCOM

- **Component Object Model**
- **Distributed Component Object Model**
  - **From Microsoft**
  - **Allows objects written in different OOP languages to communicate**
  - **Assemble a program by connecting components together like puzzle pieces**
  - **Includes ActiveX objects and Object Linking and Embedding (OLE)**
- **COM and DCOM are being supplanted by Microsoft.NET**

CORBA

- **Common Object Request Broker Architecture**
- **Open vendor-neutral framework**
- **Competes with Microsoft's proprietary DCOM**
- **Objects communicate via *Interface Definition Language (IDL)***

Object-Oriented Analysis (OOA) & Object-Oriented Design (OOD)

- **Object-Oriented Analysis (OOA)**
  - **Analyzes a *problem domain***
  - **Identifies all objects and interactions**
- **Object-Oriented Design (OOD)**
  - **Then develops the solution**

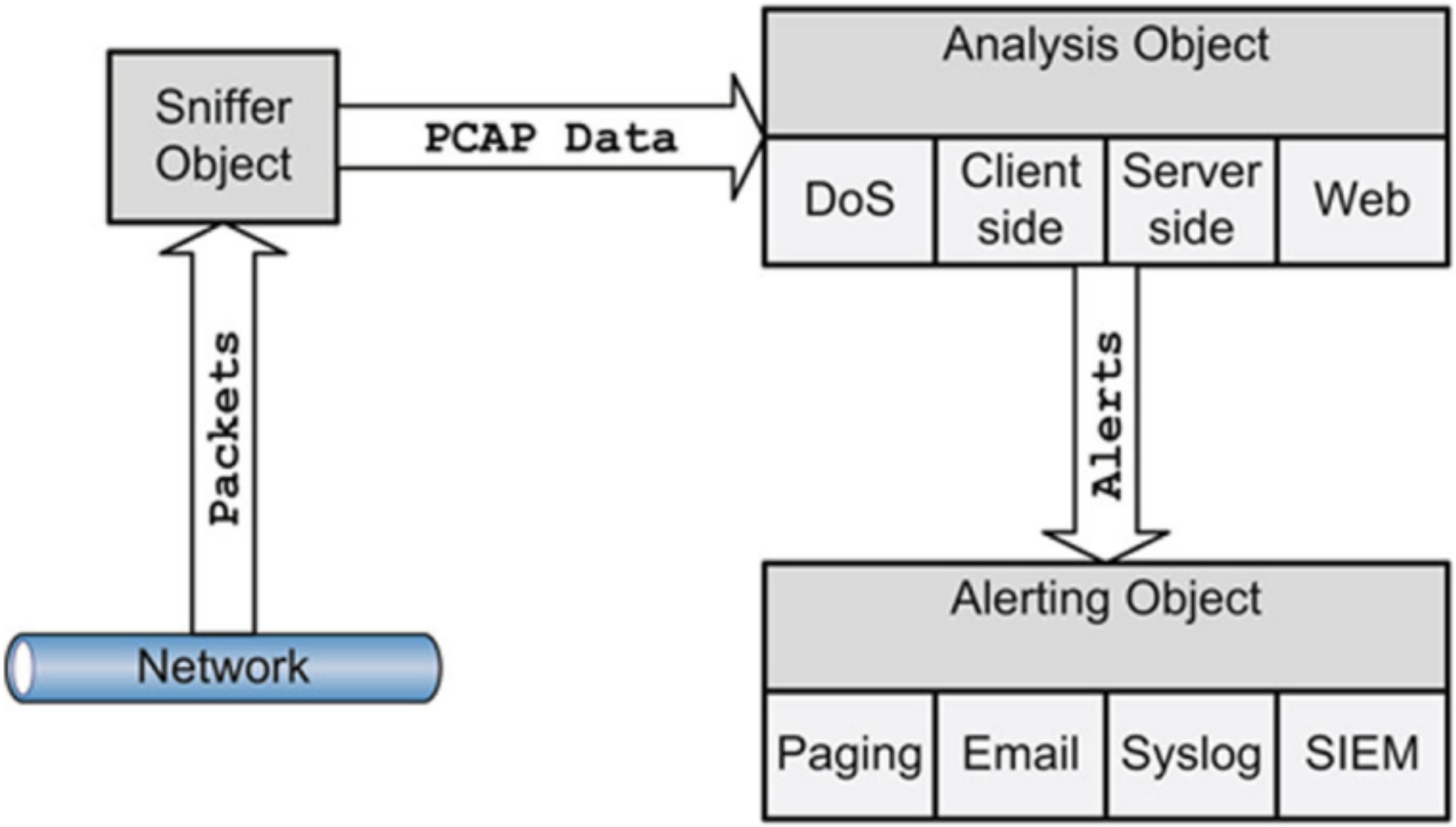


FIGURE 9.10 OOD NIDS Design

Assessing the Effectiveness of Software Security

Software Vulnerabilities

- **15-50 errors per 1000 lines of code**
- **Windows Vista has 50 million lines of code**

Types of Software Vulnerabilities

- **Hard-coded credentials**
- **Buffer overflow**
- **SQL injection**
- **Directory path traversal**
- **PHP Remote File Inclusion**

Buffer Overflow

- **Program reserves space for a variable**
  - **Ex: name[20]**
- **User submits data that's too long to fit**
- **Data written beyond the reserved space and corrupts memory**
- **Can lead to Remote Code Execution**

TOCTOU / Race Conditions

- **Time of Check/Time of Use (TOCTOU) attacks (also called Race Conditions)**
  - **A brief time of vulnerability**
  - **Attacker needs to "win the race"**

Cross-Site Scripting (XSS)

- **Insert Javascript into a page**
  - **For example, a comment box**
- **The code executes on another user's machine**
- **BeEF (Browser Exploitation Framework)**
  - **Allows an attacker to control targets' browsers**

Cross-Site Request Forgery (CSRF)

- **Trick a user into executing an unintended action**
- **With a malicious URL**
- **Or by using a stolen cookie**

```
<img src="https://bank.example.com/transfer-money?from=WHITEHAT&to=BLACKHAT">
```

Privilege Escalation

- **Vertical escalation**
  - **Attacker increases privilege level**
  - **To "Administrator", "root", or "SYSTEM"**
- **Horizontal escalation**
  - **To another user's account**

Backdoor

- **Shortcut into a system, bypassing security checks like username/password**
- **May be through exploiting a vulnerability**
- **Or a backdoor account left in the system by its developer**

Disclosure

- **Actions taken by a security researcher after finding a software vulnerability**
- **Full Disclosure**
  - **Release all details publicly**
- **Responsible Disclosure**
  - **Tell vendor privately**
  - **Give them time to patch it**

Software Capability Maturity Model (CMM)

- **From Carnegie Mellon**
- **A methodical framework for creating quality software**

Five Levels of CMM

1. **Initial - ad-hoc & chaotic**
   - **Depends on individual effort**
2. **Repeatable - basic project management**
3. **Defined**
   - **Documented standardized process**
4. **Managed**
   - **Controlled, measured process & quality**
5. **Optimizing**
   - **Continual process improvement**

Acceptance Testing

- **ISTQB (International Software Testing Qualifications Board) has 4 levels**
  - **User acceptance test**
  - **Operational acceptance test**
  - **Contract acceptance testing**
  - **Compliance acceptance testing**

Security Impact of Acquired Software

- **Commercial Off-the-Shelf (COTS) Software**
  - **Compare vendor claims with third-party research**
  - **Consider vendors going out of business, and support**
- **Custom-Developed Third Party Products**
  - **Service Level Agreements (SLA) are vital**

Artificial Intelligence

Expert Systems

- **Two components**
  - **Knowledge Base**
    - **If/then statements**
    - **Contain rules that the expert system uses to make decisions**
  - **Inference Engine**
    - **Follows the tree formed by the knowledge base**

Multi-Layer Artificial Neural Network

- **Simulates real brains**

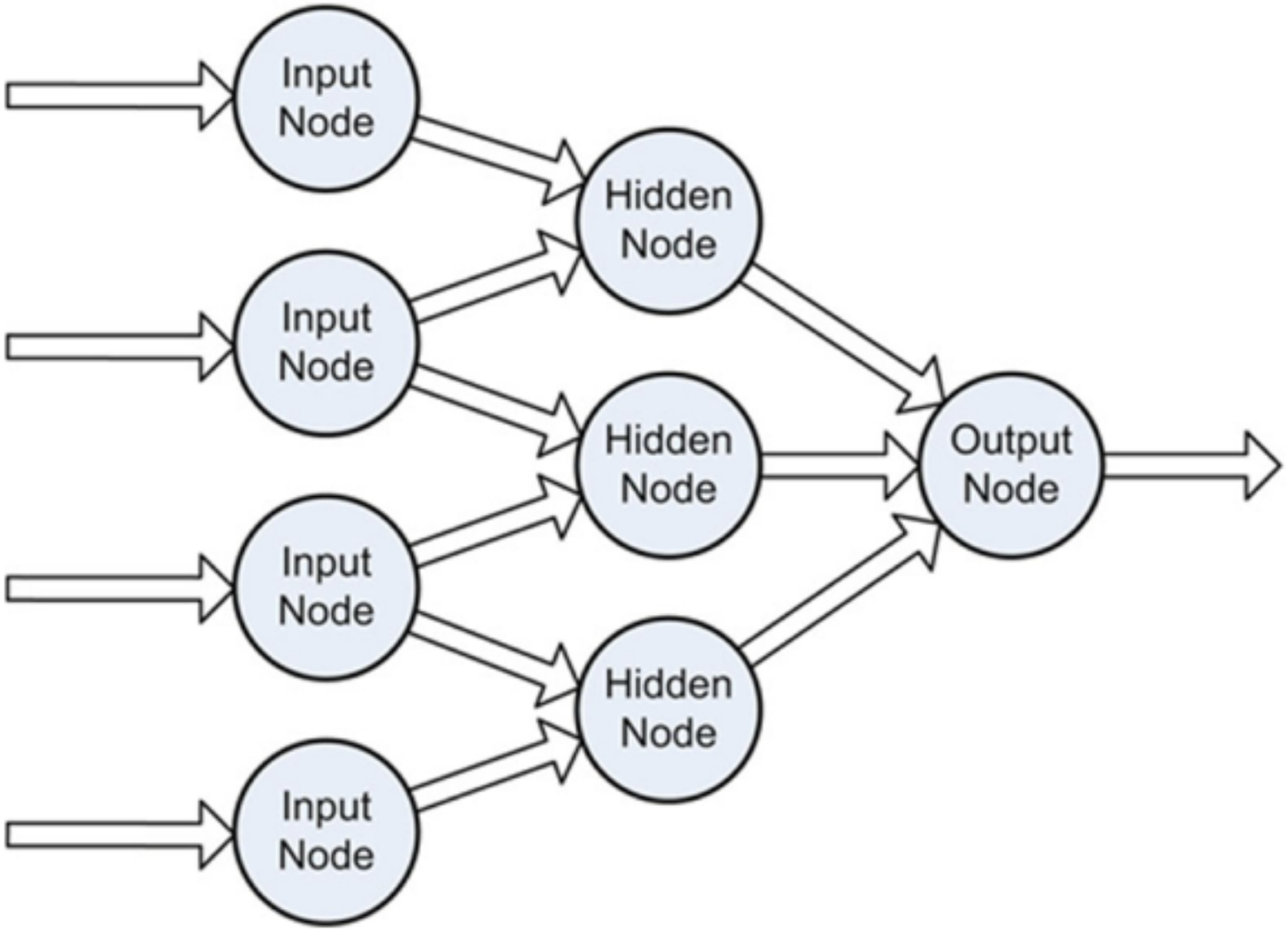


FIGURE 9.11 **Multi-Layer Artificial Neural Network**

Bayesian Filtering

- **Looks for probabilities of words in spam v. good email**

Genetic Algorithms and Programming

- **Simulates evolution**

- "Generate an initial population of random computer programs
- Execute each program in the population and assign it a fitness value according to how well it solves the problem.
- Create a new population of computer programs.
  - Copy the best existing programs
  - Create new computer programs by mutation.
  - Create new computer programs by crossover (sexual reproduction)"