CISSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 8

Software Development Security

INSIDE CLOUD AND SECURITY

WHAT'S NEW IN DOMAIN 8?

8.2 Identify and apply security controls in software development ecosystems

- Programming languages
- Libraries
- Tool sets
- Integrated Development Environment (IDE)
- Runtime
- Code repositories
- Continuous Integration and Continuous Delivery (CI/CD)
- Security Orchestration, Automation, and Response (SOAR)
- Software Configuration Management (SCM)

NEW topics in existing sub-domain

how do you handle source code securely?

Code Repositories

This is where source code and related artifacts (such as libraries) are stored

- ✓ Do not commit sensitive information
- ✓ Protect access to your code repositories
- ✓ Sign your work
- ✓ Keep your development tools (IDE) up-to-date

Integrated Development Environment

Most code repositories today use **Git**, the worlds most widely used modern version control system

CODE LIBRARIES

code libraries for some important core functions can improve application security and reduce risk

For Example:

Certain languages are prone to certain types of attacks

In lower-level languages (like C) use of safe memory allocation and string manipulation libraries can reduce risk of buffer overflow attacks

others? encryption, handling secrets, bulk data transfer

DEVOPS AND DEVSECOPS

Runtime

describes the period of time during which a software program is running

this is when dynamic application security testing (DAST) evaluates security of an application

assessing software security at runtime is generally the only option for purchased software

both source code and runtime scan is a best practice

for containers, scan images at build time and runtime

DEVOPS AND DEVSECOPS

CI/CD

Continuous Integration,
Continuous Delivery

implement identity and access management (including MFA)

store secrets securely and scan code to ensure no hard-coded secrets

Implement role-based access control (and least privilege access) to the environment

automate vulnerability scanning in your CI/CD pipeline

release versioning will improve recoverability and issues tracking

CONFIGURATION MANAGEMENT

tracks the way that systems are set up:
hardware and software (OS and applications)

SCM
Software Configuration Management

Baselining is an important component of configuration management.

a baseline is a snapshot of a system or application at a given point in time

should also create **artifacts** that may be used to help understand system configuration

system and component-level **versioning**

applications depend on compute resources and software components

DEVOPS AND DEVSECOPS

Static
Application Security Testing

analysis of computer software performed without actually executing programs

tester has access to the underlying framework, design, and implementation

tests "inside out"

requires source code

Dynamic
Application Security Testing

a program which communicates with a web application (executes the application).

tester has no knowledge of the technologies or frameworks that the application is built on

tests "outside in"

no source code required

Exam Outline

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

8.2 Identify and apply security controls in development ecosystems

8.3 Assess the effectiveness of software security

8.4 Assess security impact of acquired software

8.5 Define and apply secure coding guidelines and standards

know the basic architecture of RDBMS

Tables (relations)

contains a number of attributes, or fields. Each attribute corresponds to a column in the table.

Rows (records/tuples)

a data record within a table. Each row, which represents a complete record of specific item data, holds different data within the same structure.

Columns (fields/attributes)

a set of data values of a particular type, one value for each row of the database.

know the basic architecture of RDBMS

table

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

row

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

column

Company ID	Company Name	Address	City	State	ZIP Code	Telephone	Sales Rep
1	Acme Widgets	234 Main Street	Columbia	MD	21040	(301) 555-1212	14
2	Abrams Consulting	1024 Sample Street	Miami	FL	33131	(305) 555-1995	14
3	Dome Widgets	913 Sorin Street	South Bend	IN	46556	(574) 555-5863	26

know the basic architecture of RDBMS

Candidate Keys one or more per table

a subset of attributes that can be used to uniquely identify any record in a table. No two records in the same table will ever contain the same values for all attributes composing a candidate key.

Primary Keys one per table, set by designer

selected from the set of candidate keys for a table to be used to uniquely identify the records in a table. Each table has only one primary key, selected by the database designer from the set of candidate keys.

Foreign Keys

used to enforce relationships between two tables, also known as ***referential integrity.*** Referential integrity ensures that if one table contains a foreign key, it corresponds to a still-existing primary key in the other table in the relationship.

know the basic architecture of RDBMS

Foreign Key (example)

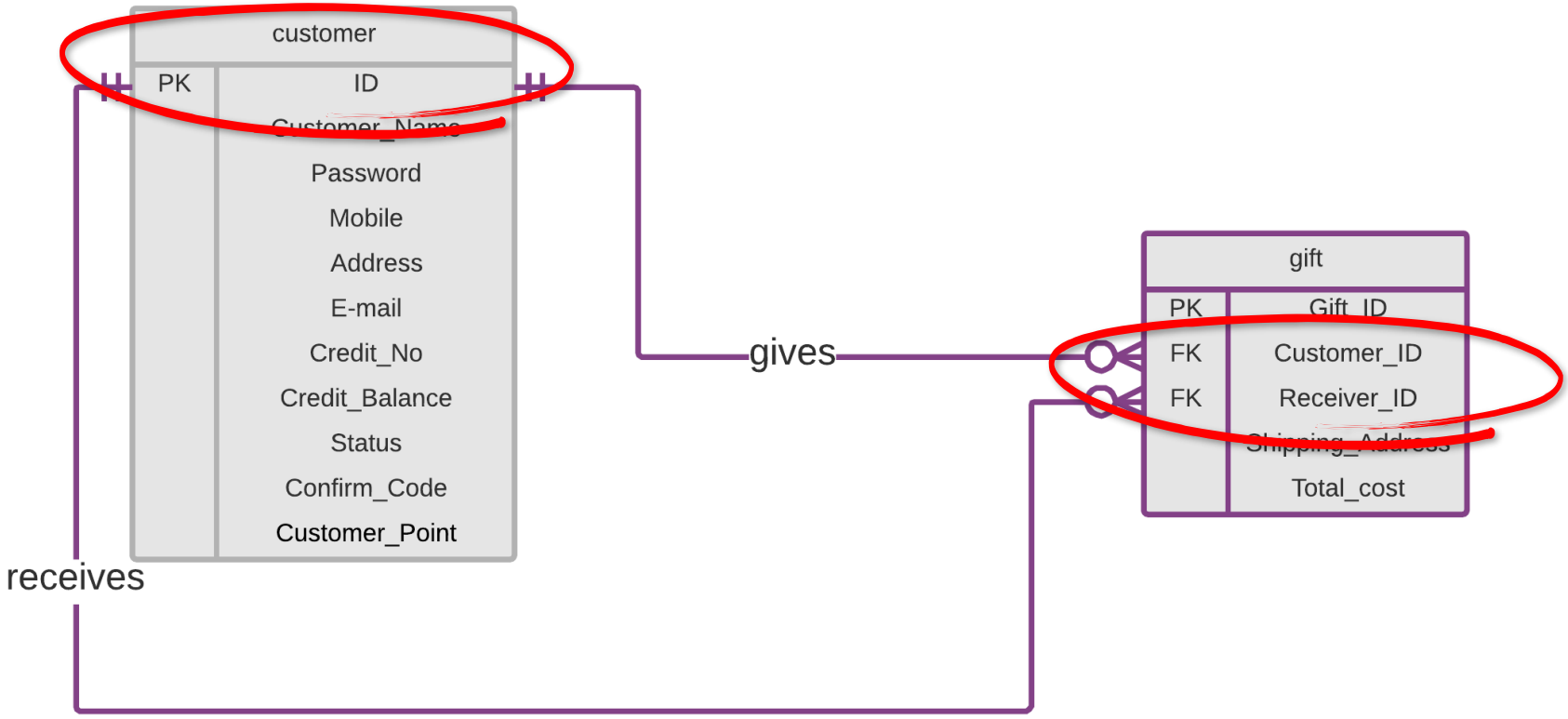


image credit: stackoverflow.com

know the basic architecture of RDBMS

Candidate Keys
one or more per table

a subset of attributes that can be used to uniquely identify any record in a table. No two records in the same table will ever contain the same values for all attributes composing a candidate key.

Primary Keys
one per table, set by designer

selected from the set of candidate keys for a table to be used to uniquely identify the records in a table. Each table has only one primary key, selected by the database designer from the set of candidate keys.

Foreign Keys

used to enforce relationships between two tables, also known as ***referential integrity.*** Referential integrity ensures that if one table contains a foreign key, it corresponds to a still-existing primary key in the other table in the relationship.

Common RDBMS threats include **aggregation** and **inference** attacks

RDBMS THREATS AND VULNERABILITIES

Aggregation | the ability to create sensitive information by combining non-sensitive data from separate sources.

Need-to-know, and least privilege can prevent this attack

Inference | the ability to deduce or assume sensitive information from observing non-sensitive pieces of information.

Blurring data and database partitioning may prevent this attack

Other attacks on RDBMS (discussed previously) include **SQL injection, TOC/TOU, backdoor**, and **DoS**.

DOMAIN 8: TYPES OF STORAGE

know types of storage, relative cost, and performance

Primary (or "real") memory

consists of the main memory resources directly available to a system's CPU. Normally consists of volatile RAM and is usually the most high-performance storage available.

Secondary storage

consists of more inexpensive, nonvolatile storage resources available to a system for long-term use. Include magnetic and optical media, such as tapes, disks, hard drives, flash drives, and compact disc/ digital versatile disc (CD/DVD) storage.

Virtual memory

allows a system to simulate additional primary memory resources through the use of secondary storage.

example: a system low on RAM makes a hard disk available for direct CPU addressing.

DOMAIN 8: TYPES OF STORAGE

know types of storage, relative cost, and performance

Virtual storage

allows a system to simulate secondary storage resources through the use of primary storage. Most common example is RAM disk that presents itself to the operating system as a secondary storage device but is actually implemented in volatile RAM.

provides a very fast file system for apps but no recovery capability.

Random access storage

allows the operating system to request contents from any point within the media.

RAM and hard drives

Sequential access storage

requires scanning through the entire media from the beginning to reach a specific address.

A common example is magnetic tape

DOMAIN 8: TYPES OF STORAGE

know types of storage, relative cost, and performance

Volatile storage

loses its contents when power is removed from the resource.

RAM is the most common example

Nonvolatile storage

does not depend upon the presence of power to maintain its contents.

Magnetic/optical media and nonvolatile RAM (NVRAM)

MACHINE LEARNING AND NEURAL NETWORKS

Expert Systems

consist of two main components: a knowledge base that contains a series of "if/ then" rules and an inference engine that uses that information to draw conclusions about other data.

Machine Learning

techniques that attempt to algorithmically discover knowledge from datasets.

Neural Networks

simulate function of the human mind by arranging a series of layered calculations to solve problems. Require extensive training on a particular problem before they can offer solutions

SYSTEMS DEVELOPMENT MODULES

Agile

place an emphasis on the needs of the customer and quickly developing new functionality that meets those needs in an iterative fashion.

Waterfall

describes a sequential development process that results in the development of a finished product.

Spiral

uses several iterations of waterfall model to produce a number of fully specified and tested prototypes.

AGILE MODEL

model for software development
based on the following four principles

Individuals and interactions over processes and tools

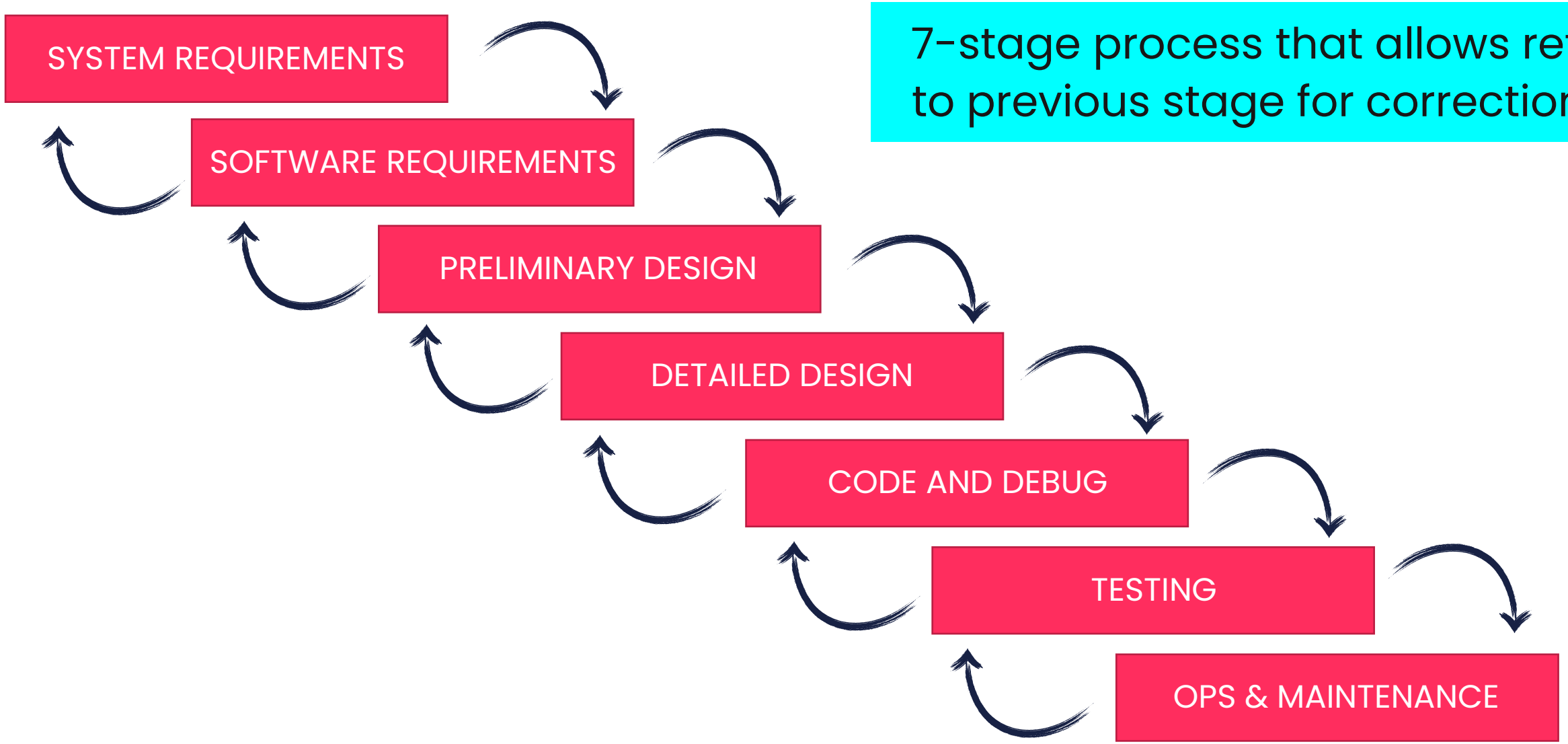
Working software over comprehensive documentation

Customer collaboration over contract negotiation

Responding to change over following a plan

First described in the Manifesto for Agile Software Development (http://agilemanifesto.org) in 2001.

WATERFALL MODEL



7-stage process that allows return to previous stage for corrections

SPIRAL MODEL

lifecycle model that allows for multiple iterations of a waterfall-style process.

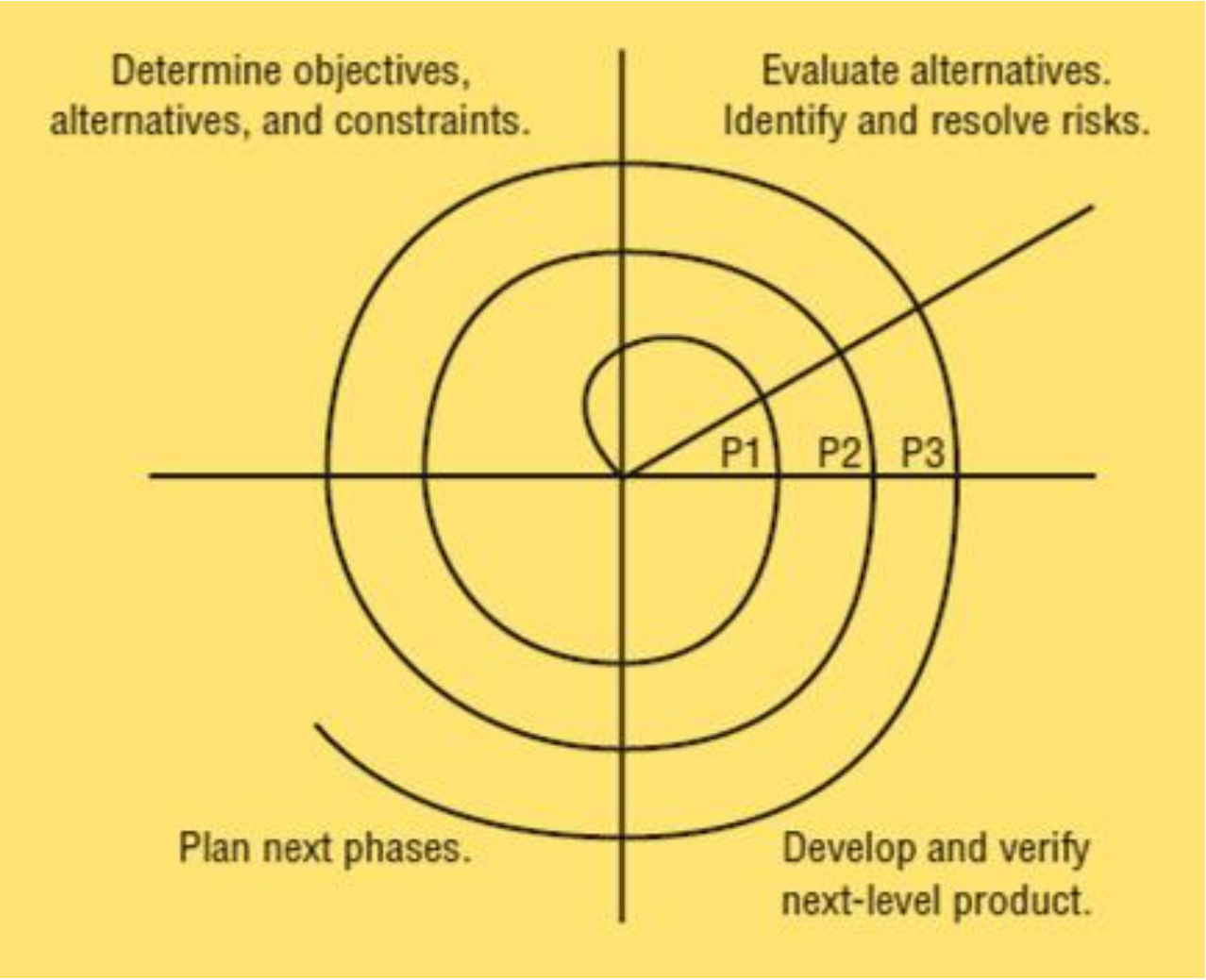
known as a *metamodel* , or a “model of models.”

each “loop” of the spiral results in the development of a new system prototype

provides a solution to the major criticism of the waterfall model:

it allows developers to return to the planning stages as demands change

in a word - "iterative"



SOFTWARE DEVELOPMENT MATURITY MODELS

help software organizations improve maturity and quality of their software processes by implementing an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes

know SW-CMM and IDEAL models for the exam

CAPABILITY MATURITY MODEL (SW-CMM)

a 5-step model for measuring software development orgs

Level 1: Initial
No plan.

Level 2: Repeatable.
Basic lifecycle mgmt.

Level 3: Defined.
Formal, documented SW development processes.

Level 4: Managed.
Quantitative measures to gain detailed understanding.

Level 5: Optimized. CI/CD
Continuous development process, w/ feedback loops.

IDEAL MODEL

model for software development which implements many of the SW-CMM attributes

Initiating. Business reasons outlined, support & infrastructure for initiative put in place.

Diagnosing. Engineers analyze current state of org & make recommendations for change.

Establishing. Org takes recommendations & develops plan to achieve those changes.

Acting. Plan put into action. Org develops solutions, tests, refines & implements

Learning. Org continuously analyzes efforts and results, proposes new actions to drive better results.

CHANGE AND CONFIGURATION MANAGEMENT

Role of change and configuration management in software development

Request Control

provides an organized framework within which users can request modifications, managers can conduct cost/benefit analysis, and developers can prioritize tasks.

Change Control

used by developers to re-create the situation encountered by the user and analyze the appropriate changes to remedy the situation.

Release Control

changes = code changes

Once the changes are finalized, they must be approved for release through the release control procedure. Should also include acceptance testing to ensure that any alterations are understood and functional

SOFTWARE TESTING

thoroughly test any software before distributing it internally (or releasing it to market). The programming team should develop special data sets that exercise all paths of the software to the fullest extent possible

some tests may be automated, and others manual

VIRUS PROPAGATION TECHNIQUES

Viruses use four main propagation techniques

File Infection

.exe and .com on Windows

infect different types of executable files and trigger when the operating system attempts to execute them.

Service injection

escape detection by injecting themselves into trusted runtime processes of the operating system, such as svchost.exe, winlogin.exe, and explorer.exe.

Boot Sector Infection

infect the legitimate boot sector and are loaded into memory during the operating system load process.

Macro Infection

Infect and spread through code in macros (often using Visual Basic for Apps in MS Office docs)

ANTIVIRUS SOFTWARE

use signature-based detection algorithms to look for telltale patterns of known viruses. It is critical signatures are updated frequently.

ANTIVIRUS SOFTWARE

Today, many use behavior-based detection monitoring target systems for unusual activity and either blocking it or flagging it, even if the software does not match a known malware signature.

TECHNIQUES TO COMPROMISE PASSWORD SECURITY

Password Crackers

designed to take credential data stolen in a data breach or other hack and extract passwords from it.

Dictionary Attacks

uses a large dictionary file with thousands of words and then runs an encryption function against all words to obtain their encrypted equivalents.

Social Engineering Attacks

consists of simply calling the user and asking for their password or posing as a technical support representative or other authority figure who needs the information immediately.

Rootkit (escalation of privilege)

freely available on the internet, used as a 2nd step by attackers exploit known vulnerabilities in various operating systems enabling attackers to elevate privilege.

APPLICATION ATTACKS

attacks attackers use to exploit **poorly written software**.

Buffer Overflow

exist when a developer does not validate user input to ensure that it is of an appropriate size (allows Input that is too large can "overflow" memory buffer)

Back Door

often used during development and debugging

undocumented command sequences that allow individuals with knowledge of the back door to bypass normal access restrictions

Time-of-Check-to-Time-of-Use

a timing vulnerability that occurs when a program checks access permissions too far in advance of a resource request.

Rootkit (escalation of privilege)

freely available on the internet and exploit known vulnerabilities in various operating systems enabling attackers to elevate privilege.

WEB APPLICATION VULNERABILITIES

used to compromise web front-end and backend databases

Cross-site scripting (XSS) occur when web apps contain 'reflected input'

A type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.

Occur when an attacker uses a web application to send malicious code to a different end user.

SQL injection attacks

Use unexpected input to a web application to gain unauthorized access to an underlying database.

NETWORK RECONNAISSANCE TECHNIQUES

techniques used by attackers preparing to attack a network

IP Probes

Automated tools simply attempt to ping each address in a range. Systems that respond to the ping request are logged for further analysis

Port Scans

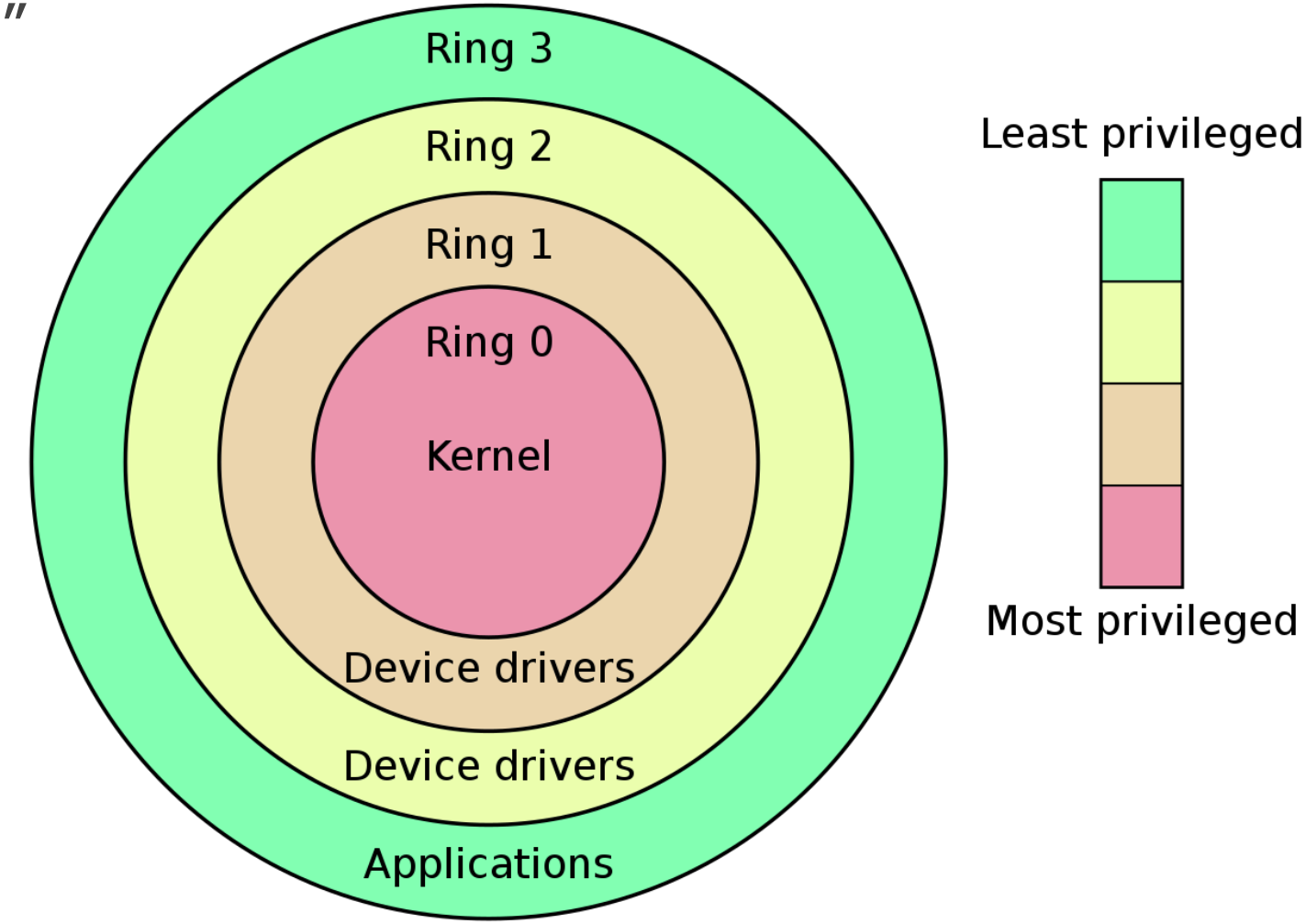
Scans a system for open/listening ports. Often, web servers, file servers, and other servers supporting critical operations are prime targets

Vulnerability Scans

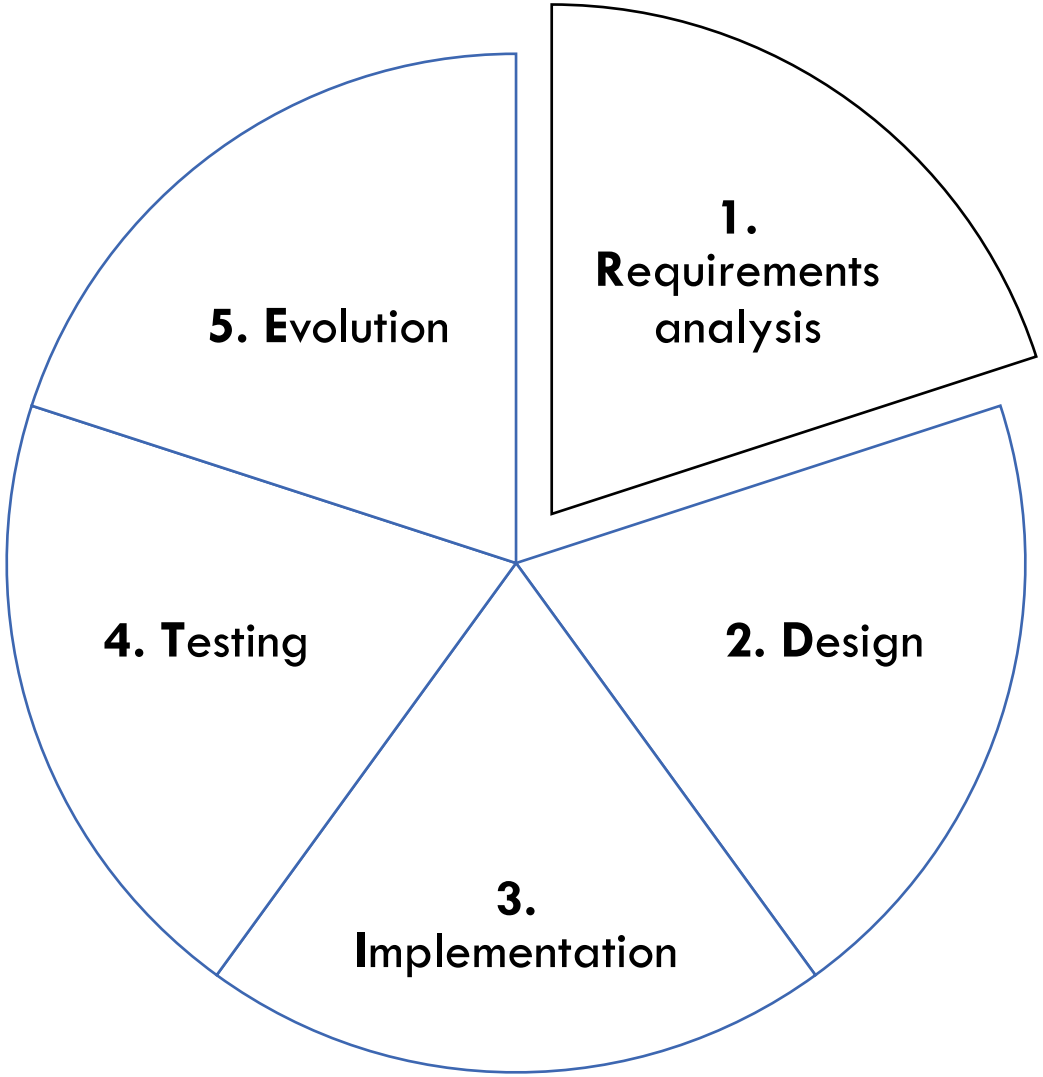
Used discover specific vulnerabilities in a system. popular tools for this purpose include Nessus, OpenVAS, Qualys, Core Impact

PROTECTION RINGS

aka “hierarchical protection domains”



THE SOFTWARE DEVELOPMENT LIFECYCLE



Real

Developers

Ideas

Take

Effort

CONCENTRIC CIRCLE SECURITY

several mutually independent security applications, processes, or services that operate toward a single common goal.

avoids a monolithic security stance

every individual security mechanism has a flaw or a workaround

intelligent combination of countermeasures (layered defense) will resist significant and persistent attempts of compromise.

Concentric circle security represents a "layered defense" aka **defense in-depth**.

ACQUIRED SOFTWARE SECURITY IMPACT

Operating system Attacks

attackers always try to search for operating system vulnerabilities, like buffer overflow , OS bugs, unpatched operating system.

Application-Level Attacks

overflow, active content, cross-site script, denial of service, SQL injection, session hijacking , phishing.

Shrink Wrap Code Attacks

an act of exploiting holes in unpatched or poorly configured software you buy and install. Often also often contain sample scripts/code.

Misconfiguration Attacks

target poorly configured service or device, or one left in default configuration (like WiFi router left in default settings).