



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](#).

#MissionBeforeMoney



# 2021 CISSP MENTOR PROGRAM

---

Class 11 – May 24<sup>th</sup>, 2021

## Instructor:

- Ryan Cloutier, Principal Security Consultant SecurityStudio



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# ALMOST THERE...

Two more classes of content, then practice.

I hope everyone is doing well. Looking for questions, so give me some!

- Check-in.
- How many have read Chapter 1 - 8?
- Questions? Where to go...

122 slides tonight, but who's counting?

Another laid back class tonight. Some reinforcement and some new content.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

### Questions, questions, questions...

1. What type of backup is typically obtained during the Response (aka Containment) phase of Incident Response?
  - A. Incremental
  - B. Full
  - C. Differential
  - D. Binary



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

## Questions, questions, questions...

1. What type of backup is typically obtained during the Response (aka Containment) phase of Incident Response?
  - A. Incremental
  - B. Full
  - C. Differential
  - D. **Binary**



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

Questions, questions, questions...

2. What is the primary goal of disaster recovery planning (DRP)?
- A. Integrity of data
  - B. Preservation of business capital
  - C. Restoration of business processes
  - D. Safety of personnel



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

Questions, questions, questions...

2. What is the primary goal of disaster recovery planning (DRP)?
- A. Integrity of data
  - B. Preservation of business capital
  - C. Restoration of business processes
  - D. **Safety of personnel**



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

## Questions, questions, questions...

3. What business process can be used to determine the outer bound of a Maximum Tolerable Downtime?
- A. Accounts receivable
  - B. Invoicing
  - C. Payroll
  - D. Shipment of goods



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

## Questions, questions, questions...

3. What business process can be used to determine the outer bound of a Maximum Tolerable Downtime?
- A. Accounts receivable
  - B. Invoicing
  - C. **Payroll**
  - D. Shipment of goods





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

## Questions, questions, questions...

4. Your Maximum Tolerable Downtime is 48 hours. What is the most cost effective alternate site choice?
- A. Cold
  - B. Hot
  - C. Redundant
  - D. Warm



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

## QUIZ...

## Questions, questions, questions...

4. Your Maximum Tolerable Downtime is 48 hours. What is the most cost effective alternate site choice?
- A. Cold
  - B. Hot
  - C. Redundant
  - D. **Warm**



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

## Questions, questions, questions...

5. A structured walkthrough test is also known as what kind of test?
- A. Checklist
  - B. Simulation
  - C. Tabletop Exercise
  - D. Walkthrough Drill



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

Questions, questions, questions...

5. A structured walkthrough test is also known as what kind of test?
- A. Checklist
  - B. Simulation
  - C. **Tabletop Exercise**
  - D. Walkthrough Drill



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

## Questions, questions, questions...

6. Which type of backup will include only those files that have changed since the most recent Full backup?
- A. Full
  - B. Differential
  - C. Incremental
  - D. Binary



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# QUIZ...

## Questions, questions, questions...

6. Which type of backup will include only those files that have changed since the most recent Full backup?
- A. Full
  - B. Differential**
  - C. Incremental
  - D. Binary



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

**LET'S DO THIS!**

More incident management...

## CHAPTER

## 8

Domain 7: Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

Where we left off, we had just talked about incident management/response...

Page 411



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Executive Succession Planning

- Organizations must ensure that there is always an executive available to make decisions during a disaster
- A common mistake is allowing entire executive teams to be offsite at distant meetings
- One of the simplest executive powers is the ability to endorse checks and procure money.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Plan Approval

- Now that the initial BCP/DRP plan has been completed, senior management approval is the required next step
- It is ultimately senior management's responsibility to protect an organization's critical assets and personnel
- Senior management must understand that they are responsible for the plan, fully understand the plan, take ownership of it, and ensure its success.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Backups and availability (again...)

- In order to be able to successfully recover critical business operations, the organization needs to be able to effectively and efficiently backup and restore both systems and data
- Verification of recoverability from backups is often overlooked
- Critical backup media must be stored offsite
- Ensure that the organization can quickly procure large high-end tape drives (if necessary)
- If the MTTR is greater than the MTD, then an alternate backup or availability methodology must be employed



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Backups and availability (again...)

#### Hardcopy Data

- Hardcopy data is any data that are accessed through reading or writing on paper rather than processing through a computer system.
- In weather-emergency-prone areas such as Florida, Mississippi, and Louisiana, many businesses develop a “paper only” DRP, which will allow them to operate key critical processes with just hard copies of data, battery-operated calculators, and other small electronics, as well as pens and pencils



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Backups and availability (again...)

#### Electronic Backups

- Archives that are stored electronically
- **Full Backups**
  - Every piece of data is copied and stored on the backup repository
  - Time consuming, bandwidth intensive, and resource intensive
  - Will ensure that any necessary data is available
- **Incremental Backups**
  - Archive data that have changed since the last full or incremental backup
- **Differential Backups**
  - Archive data that have changed since the last full backup



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Backups and availability (again...)

#### Electronic Backups

- Archives that are stored electronically
- **Electronic vaulting**
  - Batch process of electronically transmitting data that is to be backed up on a routine, regularly scheduled time interval
  - Used to transfer bulk information to an offsite facility
  - Good tool for data that need to be backed up on a daily or possibly even hourly rate
  - Stores sensitive data offsite
  - Can perform the backup at very short intervals to ensure that the most recent data is backed up
  - Occurs across the Internet in most cases (important that the information sent for backup be sent via a secure communication channel and protected through a strong encryption protocol)



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Backups and availability (again...)

#### Electronic Backups

- Archives that are stored electronically
- **Remote Journaling**
  - A database journal contains a log of all database transactions
  - May be used to recover from a database failure
  - Remote Journaling saves the database checkpoints and database journal to a remote site
- **Database shadowing**
  - Uses two or more identical databases that are updated simultaneously
  - Can exist locally, but it is best practice to host one shadow database offsite
  - Allows faster recovery when compared with remote journaling



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Software Escrow

- Maintain the availability of their applications even if the vendor that developed the software initially goes out of business
- Allow a neutral third party to hold the source code
- Should the development organization go out of business or otherwise violate the terms of the software escrow agreement, then the third party holding the escrow will provide the source code and any other information to the purchasing organization.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### DRP testing, training, and awareness

- Skipping these steps is one of the most common BCP/DRP mistakes
- A DRP is never complete, but is rather a continually amended method for ensuring the ability for the organization to recover in an acceptable manner
- Used to correct mistakes
- A DRP that will be effective will have some inherent complex operations and maneuvers to be performed by administrators
- Each member of the DRP should be exceedingly familiar with the particulars of their role in a DRP.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### DRP Testing

- In order to ensure that a Disaster Recovery Plan represents a viable plan for recovery, thorough testing is needed
- Routine infrastructure, hardware, software, and configuration changes materially alter the way in which the DRP needs to be carried out
- Ensure both the initial and continued efficacy of the DRP as a feasible recovery methodology, testing needs to be performed.
- Different types of tests
- At an minimum, regardless of the type of test selected, tests should be performed on an annual basis



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### DRP Testing

#### DRP Review

- Most basic form of DRP testing
- Focused on simply reading the DRP in its entirety to ensure completeness of coverage
- Typically performed by the team that developed the plan, and will involve team members reading the plan in its entirety to quickly review the overall plan for any obvious flaws



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### DRP Testing

#### Checklist

- Also known as consistency testing
- Lists all necessary components required for successful recovery, and ensures that they are, or will be, readily available should a disaster occur
- Often performed concurrently with the structured walkthrough or tabletop testing as a first testing threshold
- Focused on ensuring that the organization has, or can acquire in a timely fashion, sufficient resources on which their successful recovery is dependent



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### DRP Testing

#### Parallel Processing

- Common in environments where transactional data is a key component of the critical business processing
- Typically involves recovery of critical processing components at an alternate computing facility, and restore data from a previous backup
- Regular production systems are not interrupted
- Transactions from the day after the backup are then run against the newly restored data, and the same results achieved during normal operations for the date in question should be mirrored by the recovery system's results
- Organizations that are highly dependent upon mainframe and midrange systems will often employ this type of test.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### DRP Testing

#### Partial and Complete Business Interruption

- This type of test can actually be the cause of a disaster, so extreme caution should be exercised before attempting an actual interruption test
- Testing will include having the organization stop processing normal business at the primary location, and instead leverage the alternate computing facility
- More common in organizations where fully redundant, load-balanced, operations exist



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Training

- An element of DRP training comes as part of performing the tests
- More detailed training on some specific elements of the DRP process may be required.

### Starting Emergency Power

- Converting a datacenter to emergency power, such as backup generators
- Specific training and testing of changing over to emergency power should be regularly performed.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Training

- An element of DRP training comes as part of performing the tests
- More detailed training on some specific elements of the DRP process may be required.

### Calling Tree Training/Test

- Individuals with calling responsibilities are expected to be able to answer within a very short time period, or otherwise make arrangements.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Awareness

Even for those members who have little active role with respect to the overall recovery process, there is still the matter of ensuring that all members of an organization are aware of the organization's prioritization of safety and business viability in the wake of a disaster.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Continued BCP/DRP maintenance

- The BCP/DRP must be kept up to date
- BCP/DRP plans must keep pace with all critical business and IT changes.

#### Change Management

- The Change Management process is designed to ensure that security is not adversely affected as systems are introduced, changed, and updated.
- Includes tracking and documenting all planned changes, formal approval for substantial changes, and documentation of the results of the completed change
- All changes must be auditable
- The change control board manages this process
- The BCP team should be a member of the change control board, and attend all meetings to identify any changes that must be addressed by the BCP/DRP plan



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### BCP/DRP Mistakes

Common BCP/DRP mistakes include:

- Lack of management support
- Lack of business unit involvement
- Lack of prioritization among critical staff
- Improper (often overly narrow) scope
- Inadequate telecommunications management
- Inadequate supply chain management
- Incomplete or inadequate crisis management plan
- Lack of testing
- Lack of training and awareness
- Failure to keep the BCP/DRP plan up to date



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Specific BCP/DRP frameworks

A handful of specific frameworks include NIST SP 800-34, ISO/IEC-27031, and BCI.

#### NIST SP 800-34

- The National Institute of Standards and Technology (NIST) Special Publication 800-34 “Contingency Planning Guide for Information Technology Systems”
- May be downloaded at <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Specific BCP/DRP frameworks

#### ISO/IEC-27031

- Draft guideline that is part of the ISO 27000 series, which also includes ISO 27001 and ISO 27002
- Focuses on BCP (DRP is handled by another framework)
- The current formal name is “ISO/IEC 27031 Information technology—Security techniques—Guidelines for ICT Readiness for Business Continuity (final committee draft).” According to <http://www.iso27001security.com/html/27031.html>, ISO/IEC 27031 is designed to:
  - “Provide a framework (methods and processes) for any organization—private, governmental, and nongovernmental;
  - Identify and specify all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organization's ISMS, helping to ensure business continuity;
  - Enable an organization to measure its continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.”



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Specific BCP/DRP frameworks

#### ISO/IEC-27031

- Terms and acronyms used by ISO/IEC 27031 include:
  - ICT—Information and Communications Technology
  - ISMS—Information Security Management System
- A separate ISO plan for disaster recovery is ISO/IEC 24762:2008, “Information technology—Security techniques—Guidelines for information and communications technology disaster recovery services.” More information is available at [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=41532](http://www.iso.org/iso/catalogue_detail.htm?csnumber=41532)



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Specific BCP/DRP frameworks

#### BS-25999

- British Standards Institution (BSI, <http://www.bsigroup.co.uk/>) released BS-25999, which is in two parts:
  - “Part 1, the Code of Practice, provides business continuity management best practice recommendations. Please note that this is a guidance document only.
  - Part 2, the Specification, provides the requirements for a Business Continuity Management System (BCMS) based on BCM best practice. This is the part of the standard that you can use to demonstrate compliance via an auditing and certification process.”<sup>14</sup>



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #7: Security Operations

### Specific BCP/DRP frameworks

#### BCI

- The Business Continuity Institute (BCI, <http://www.thebci.org/>) published a six-step Good Practice Guidelines (GPG) in 2008, latest version is 2013 which describes the Business Continuity Management (BCM) process:
  - Management Practices
    - PP1 Policy & Program Management
    - PP2 Embedding Business Continuity
  - Technical Practices
    - PP3 Analysis
    - PP4 Design
    - PP5 Implementation
    - PP6 Validation



CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

Domain #7: Security Operations

And...

**Domain #7: Security Operations (or Chapter 8) is in the bag!**

Break time?

Think again...





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

**LET'S DO THIS!**

Sooooooooo close....

## CHAPTER

## 9

Domain 8: Software  
Development Security  
(Understanding, Applying,  
and Enforcing Software  
Security)

Page 429



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

**LET'S DO THIS!**

Sooooooooo close....

CHAPTER

**OUR LAST DOMAIN!!!**

(Understanding, Applying,  
and Enforcing Software  
Security)

Page 429



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

- Programming Concepts
- Application Development Methods
- Databases
- Object-Oriented Design and Programming
- Assessing the Effectiveness of Software Security
- Artificial Intelligence



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Unique Terms & Definitions:

- **Extreme Programming (XP)**—an Agile development method that uses pairs of programmers who work off a detailed specification
- **Object**—A “black box” that combines code and data, and sends and receives messages
- **Object-Oriented Programming**—changes the older procedural programming methodology, and treats a program as a series of connected objects that communicate via messages



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Unique Terms & Definitions:

- **Procedural languages**—programming languages that use subroutines, procedures and functions
- **Spiral Model**—a software development model designed to control risk
- **Systems Development Life Cycle**—a development model that focuses on security in every phase
- **Waterfall Model**—An application development model that uses rigid phases; when one phase ends, the next begins



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

- Programmers may make 15-50 mistakes per thousand lines of code, but following a programming maturity framework such as the SEI Capability Maturity Model (CMM) can lower that number to 1 mistake per thousand.

### SEI Capability Maturity Model (CMM)

- The Software Capability Maturity Model (CMM) is a maturity framework for evaluating and improving the software development process. The model was developed by Carnegie Mellon University's (CMU) Software Engineering Institute (SEI).
- The goal of CMM is to develop a methodical framework for creating quality software which allows measurable and repeatable results



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

## LECTURE

## Domain #8: Software Development Security

- Programmers may make 15-50 mistakes per thousand lines of

Software Engineering Institute | Carnegie Mellon University

What are you looking for?

Work Areas ▾ Engage with Us Products & Services ▾ Library ▾ News Careers About Us ▾

Home > CMMI

Share Email Print

## CMMI

This information has moved to [www.cmmiinstitute.com](http://www.cmmiinstitute.com).

As part of its mission to transition mature technology to the software community, the SEI has transferred CMMI-related products and activities to the CMMI Institute, a 100%-controlled subsidiary of Carnegie Innovations, Carnegie Mellon University's technology commercialization enterprise. The CMMI Institute will conduct CMMI training and certification, sponsor conferences and classes, and provide information about CMMI process improvement models and appraisals.

The SEI will continue to pioneer and advance new research in the field of software process management. More information about our current work is available at <http://www.sei.cmu.edu/process>.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

## LECTURE

## Domain #8: Software Development Security



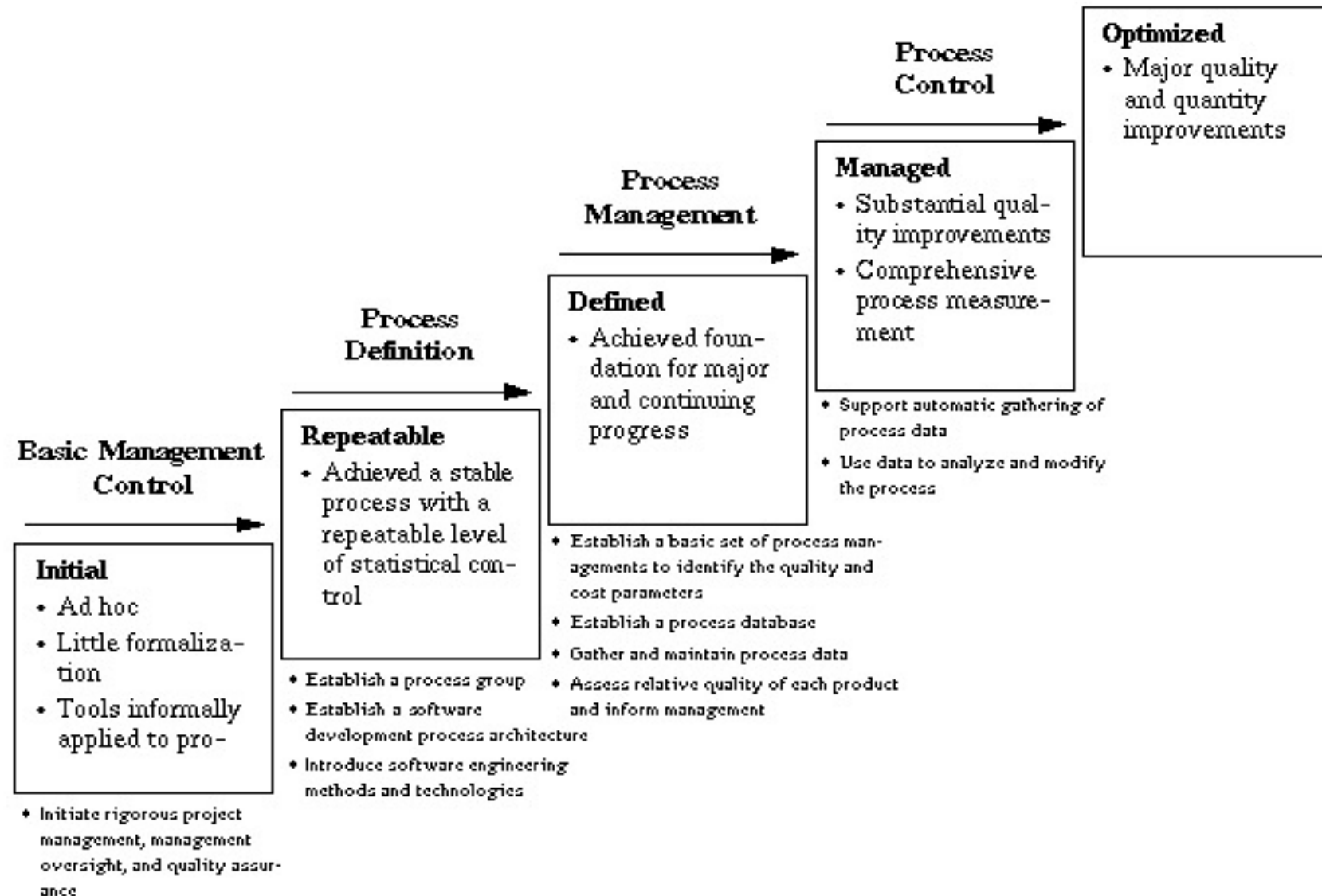




# CISSP® MENTOR PROGRAM – SESSION ELEVEN

LE  
Dor

SE





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Machine Code

- Machine code (also called machine language) is software that is executed directly by the CPU. Machine code is CPU-dependent; it is a series of 1s and 0s that translate to instructions that are understood by the CPU.

### Source Code

- Source code is computer programming language instructions which are written in text that must be translated into machine code before execution by the CPU.

# Machine Code



A good explainer video for assembly language and machine code is:

<https://youtu.be/wA2oMRmbrfo>



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

## LECTURE

## Domain #8: Software Development Security

## Source Code

```
1009
1010
1011 {
1012     // Because this packet has not been fragmented, it can be passed to the upper layer
1013     head_ip_header_data = (UCHAR *)packet->L3.IPv4Header;
1014     NnIpReceived(t, ip->SrcIP, ip->DstIP, ip->Protocol, data, size, ip->TimeToLive,
1015                 head_ip_header_data, head_ip_header_size, l3_size);
1016 }
1017 else
1018 {
1019     // This packet is necessary to combine because it is fragmented
1020     UINT offset = IPV4_GET_OFFSET(ip) * 8;
1021     IP_COMBINE *c = NnSearchIpCombine(t, ip->SrcIP, ip->DstIP, Endian16(ip->Identificati
1022
1023     if (offset == 0)
1024     {
1025         head_ip_header_data = (UCHAR *)packet->L3.IPv4Header;
1026     }
1027
1028     last_packet = ((IPV4_GET_FLAGS(ip) & 0x01) == 0 ? true : false);
1029
1030     if (c != NULL)
1031     {
1032         // To be the second or subsequent packet
1033     }
1034 }
```

Output

```
8>Copyright (C) Microsoft Corporation. All rights reserved.
7>Packet32.c
8>Linking...
9>Unix.c
9>Tracking.c
9>Tick64.c
```

(Name)	NnFragmmentedIpRecei
File	c:\tmp\v4.03-9404\src
FullName	NnFragmmentedIpRecei
IsInjected	False
IsInline	False
IsOverloaded	False
IsFixed	False

(Name)  
Sets/returns the name of the object.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Assemblers

- Assembly language is a low-level computer programming language. Assembly language instructions are short mnemonics, such as “ADD,” “SUB” (subtract), and “JMP” (jump), that match to machine language instructions. An assembler converts assembly language into machine language. A disassembler attempts to convert machine language into assembly.

### Compilers

- Compilers take source code, such as C or Basic, and compile it into machine code. Once compiled, the machine language is executed directly by the CPU.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Interpreters

- Interpreted languages differ from compiled languages: interpreted code (such as shell code) is compiled on the fly each time the program is run. Examples may include Perl, Python, Java, etc.

### Bytecode

- Bytecode, such as Java bytecode, is also interpreted code. Bytecode exists as an intermediary form (converted from source code), but still must be converted into machine code before it may run on the CPU.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Programing Language Generations

- First-generation language: machine code
- Second-generation language: assembly
- Third-generation language: COBOL, C, Basic
- Fourth-generation language: ColdFusion, Progress 4GL, Oracle Reports
  - Fourth-generation languages tend to be Graphical User Interface (GUI)-focused; dragging and dropping elements, and then generating code based on the results.
  - 4GL languages tend to be focused on the creation of databases, reports, and websites.





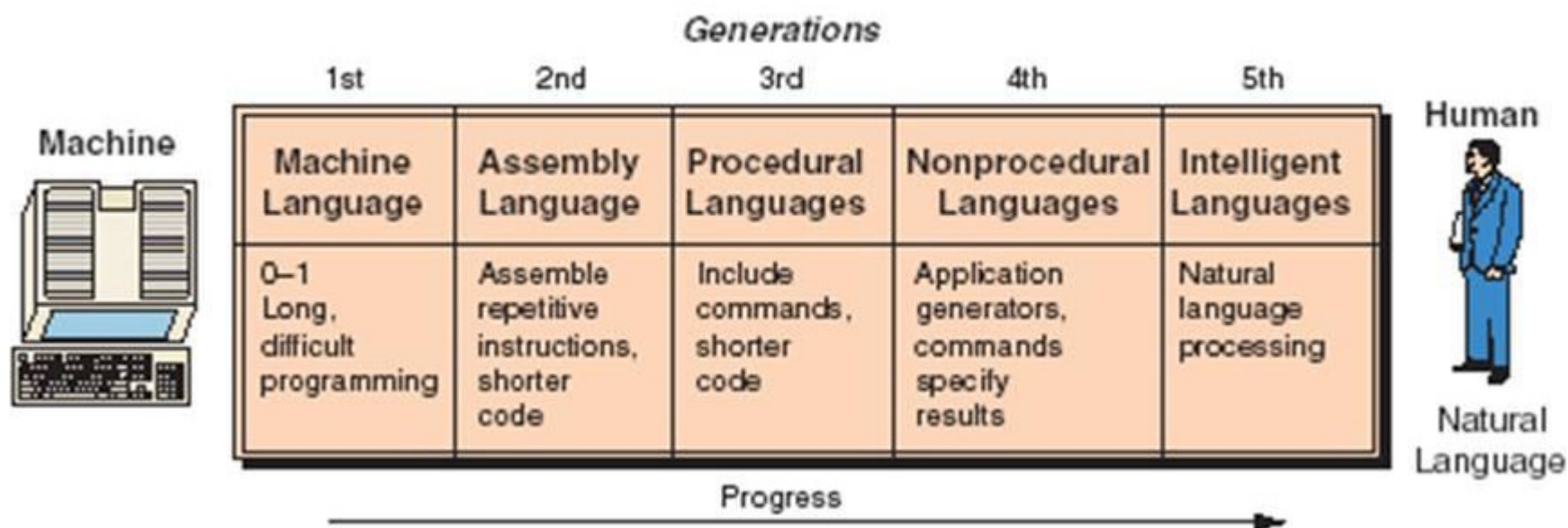
## CISSP® MENTOR PROGRAM – SESSION ELEVEN

## LECTURE

## Domain #8: Software Development Security

## Programing Language Generations

- First generation language: machine code



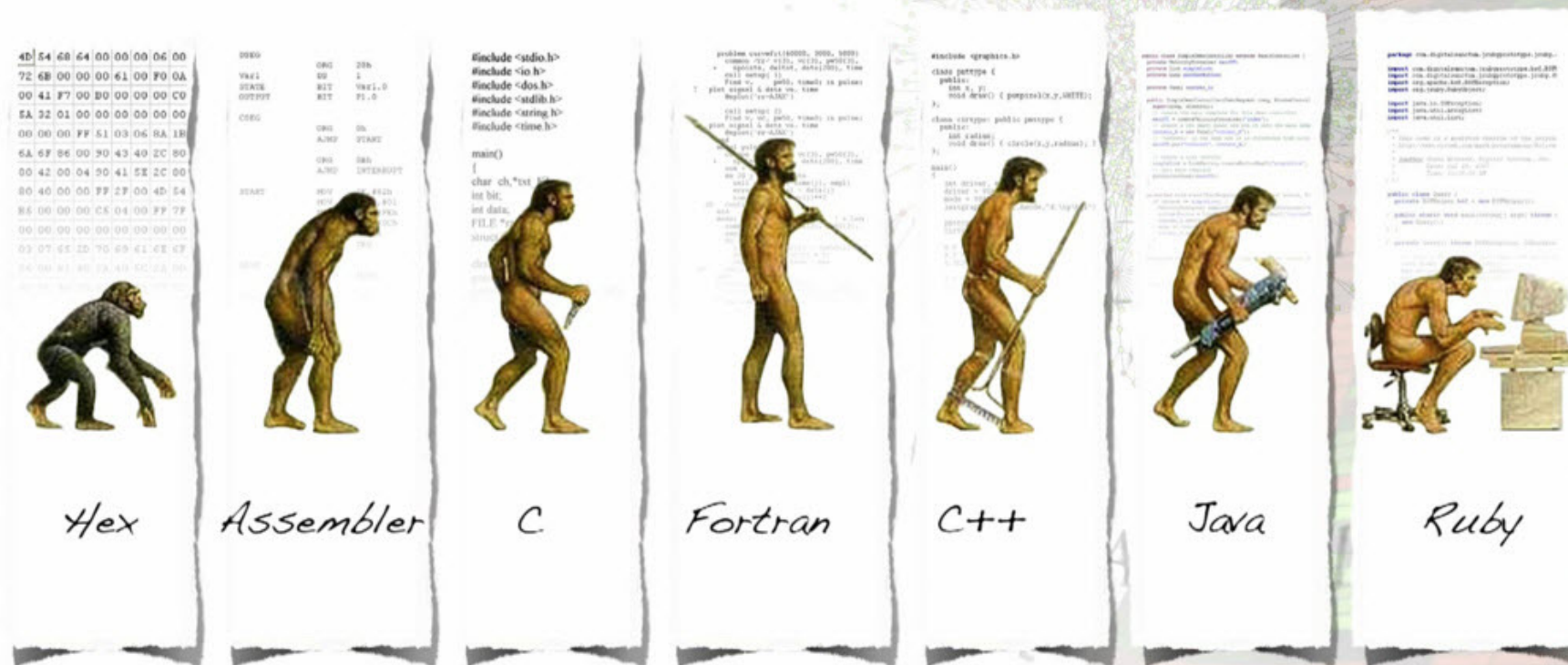


# LECTURE

## Domain #8: Software Development Security

Pi

# The Evolution Of Computer Programming Languages





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Computer-Aided Software Engineering (CASE)

Uses programs to assist in the creation and maintenance of other computer programs.

There are three types of CASE software:

1. **Tools:** support only specific task in the software-production process.
2. **Workbenches:** support one or a few software process activities by integrating several tools in a single application.
3. **Environments:** support all or at least part of the software production process with a collection of Tools and Workbenches.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Top-Down versus Bottom-Up Programming

- **Top-Down** (TD) programming starts with the broadest and highest level requirements (the concept of the final program) and works down towards the low-level technical implementation details.
- **Bottom-Up** programming is the reverse: it starts with the low-level technical implementation details and works up to the concept of the complete program.

Procedural languages such as C have historically been programmed Top-Down style: start with the main program, define the procedures, and work down from there. Object-oriented programming typically uses bottom-up design: define the objects, and use them to build up to the final program.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Types of Publicly-Released Software

- Open and Closed Source Software:
  - Closed source software is software typically released in executable form: the source code is kept confidential. Examples include Oracle and Microsoft Windows 7.
  - Open source software publishes source code publicly, allowing anyone to inspect, modify, or compile the code themselves. Examples include Ubuntu Linux and the Apache web server.
- “Closed source software” and “proprietary software” are sometimes used as synonyms, but that is not always true: some open source software is also proprietary.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Free Software, Shareware, and Crippleware:

- Free software:
  - “Free” may mean it is free of charge to use (sometimes called “free as in beer”),
  - “Free” may mean the user is free to use the software in any way they would like, including modifying it (sometimes called “free as in liberty”).
  - The two types are called **gratis** and **libre**, respectively. Freeware is “free as in beer” (gratis) software, which is free of charge to use.
- Shareware is fully-functional proprietary software that may be initially used free of charge. If the user continues to use the Shareware for a specific period of time specified by the license (such as 30 days), the Shareware license typically requires payment.
- Crippleware is partially-functioning proprietary software, often with key features disabled. The user is typically required to make a payment to unlock the full functionality.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Licensing

- Most software, both closed and open source, is protected by software licensing.
- Proprietary software is usually copyrighted the users of the software must usually agree to the terms of the software licensing agreement before using the software. These agreements are often called EULAs (End-User License Agreements), which are usually agreed to when the user clicks “I agree” while installing the software.
- Open source software may be protected by a variety of licensing agreements, including the GNU Public License (GPL), BSD (Berkeley Software Distribution), and Apache (named after the Apache Software Foundation) licenses.
- The most prevalent of open source licenses is the GPL, which focuses on free (libre) software, allowing users the freedom to use, change, and share software. The core of the GPL is the term “copyleft,” a play on copyright: copyleft seeks to ensure that free (libre) software remains free. A Quick Guide to GPLv3 (see: <http://www.gnu.org/licenses/quick-guide-gplv3.html>)



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

Soft

•

•

•

•

The screenshot shows the Creative Commons website with a search bar at the top. Below the navigation bar, there's a section titled "Discover the new CC Search" with a description: "Try the new CC image search with over 300 million images from 19 collections and easier attribution." A red button labeled "Start searching" is visible. To the right, there's a preview of the CC Search interface showing an image of grass and a detailed attribution section with a "Copy HTML" button.

free. A Quick Guide to GPLv3 (see: <http://www.gnu.org/licenses/quick-guide-gplv3.html>)






## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software

- Malware
- Licensing
- Privacy
- Mobile
- (Encryption)
- Usability
- Open Source
- Software
- For
- The
- on
- sh
- co



**GNU Operating System**  
 Sponsored by the [Free Software Foundation](#)

[JOIN THE FSF](#)  
 Free Software Supporter  
 email address  [Sign up](#)

[ABOUT GNU](#) [PHILOSOPHY](#) [LICENSES](#) [EDUCATION](#) [SOFTWARE](#) [DOCS](#) [HELP GNU](#) [More ▼](#)

### GNU General Public License

- [A Quick Guide to GPLv3](#)
- [Why Upgrade to GPLv3](#)
- [Frequently Asked Questions about the GNU licenses](#)
- [How to use GNU licenses for your own software](#)
- [Translations of the GPL](#)
- The GPL in other formats: [plain text](#), [Texinfo](#), [LaTeX](#), [standalone HTML](#), [ODF](#), Docbook [v4](#) or [v5](#), [Markdown](#), and [RTF](#).
- [GPLv3 logos](#) to use with your project
- [Old versions of the GNU GPL](#)
- [What to do if you see a possible GPL violation](#)




---

**GNU GENERAL PUBLIC LICENSE**

Version 3, 29 June 2007

free. A Quick Guide to GPLv3 (see: <http://www.gnu.org/licenses/quick-guide-gplv3.html>)





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- Waterfall Model - linear application development model that uses rigid phases; when one phase ends, the next begins.
  - Predates software design and was first used in manufacturing
  - First used to describe a software development process in 1969
  - Unmodified waterfall model does not allow developers to go back to previous steps – **NO ITERATION**



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

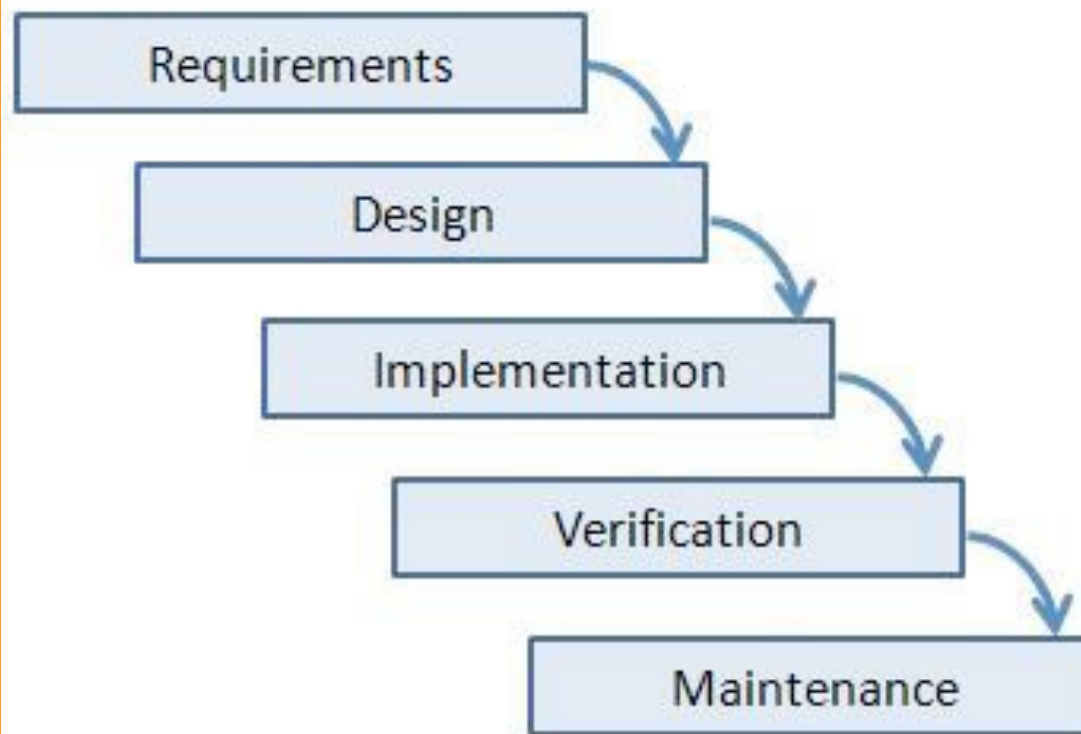
# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- Waterfall Model is a sequential model that moves from one phase to the next before moving on to the next phase.
- Predates modern manufacturing
- First used in 1969
- Unmodified, it is not back to

#### Waterfall Model





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

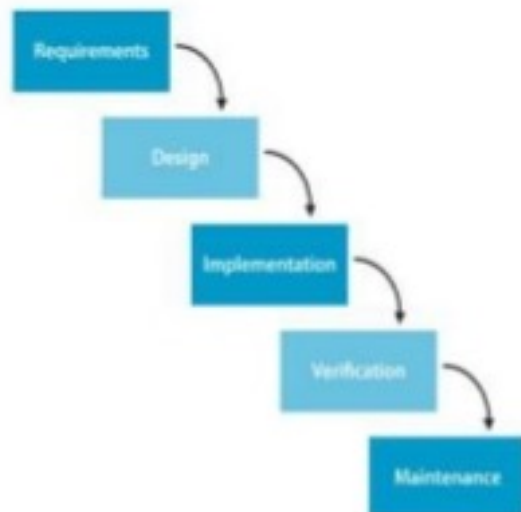
## Domain #8: Software Development Security

### Application Development Methods

- Modified Waterfall Model

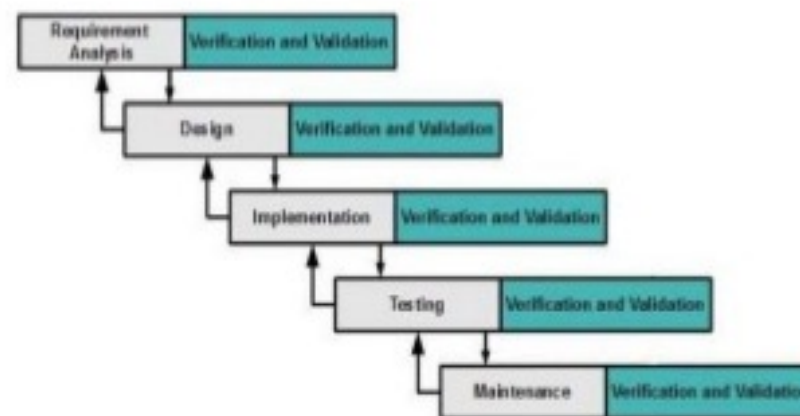
#### WATERFALL MODEL

The waterfall model has a very well structured plan & requirements to be followed. This model works well for large projects but has a longer duration period.



#### MODIFIED WATERFALL MODEL

Modified waterfall model verified & validate the user requirements for every phase. Meanwhile, waterfall did not, it only verify & validate user requirements @ the end of the phase.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- Sashimi Model
  - highly overlapping steps
  - based on (and a reaction to) the Waterfall Model
  - named after the Japanese delicacy Sashimi, which has overlapping layers of fish (and also a hint for the exam)
  - based on the hardware design model used by Fuji-Xerox



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

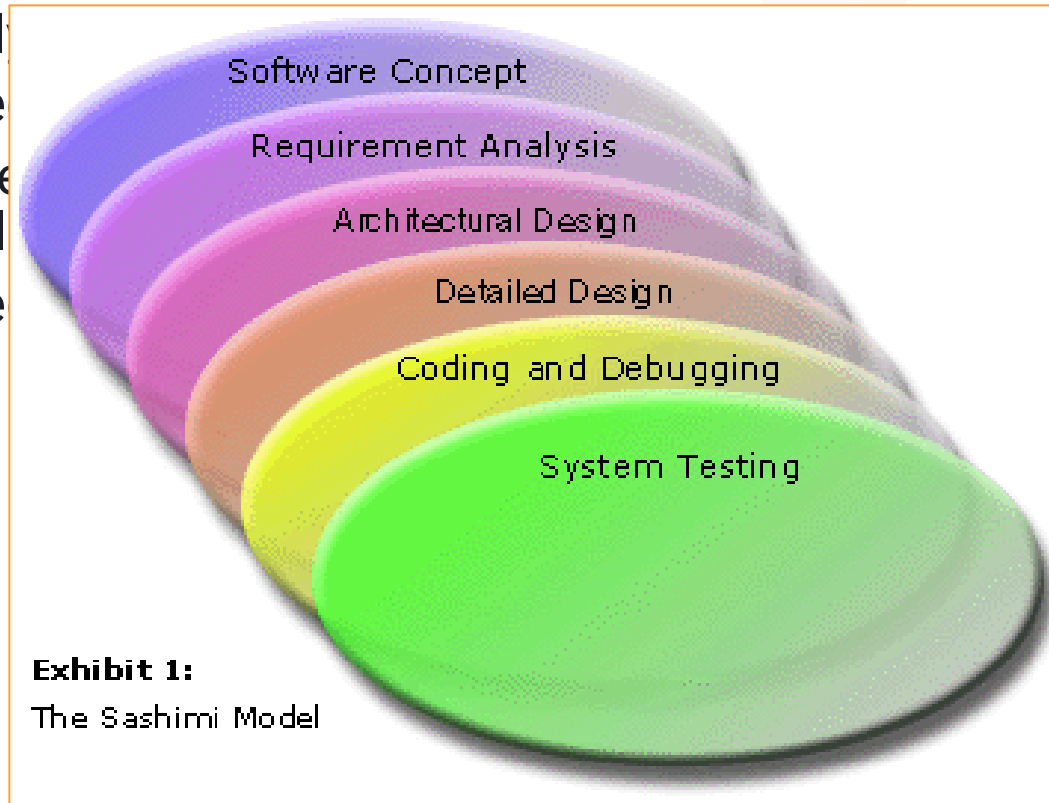
# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- Sashimi Model

- high
- base
- name
- overl
- base



n has  
xam)  
Xerox



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- Spiral
  - Described in the 1986 paper “A Spiral Model of Software Development and Enhancement” (see: <http://portal.acm.org/citation.cfm?id=12948>).
  - repeats steps of a project, starting with modest goals, and expanding outwards in ever wider spirals (called rounds).
  - each round of the spiral constitutes a project
  - each round may follow traditional software development methodology such as Modified Waterfall
  - risk analysis is performed each round



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application

- Spiral

- Describe Development

<http://>

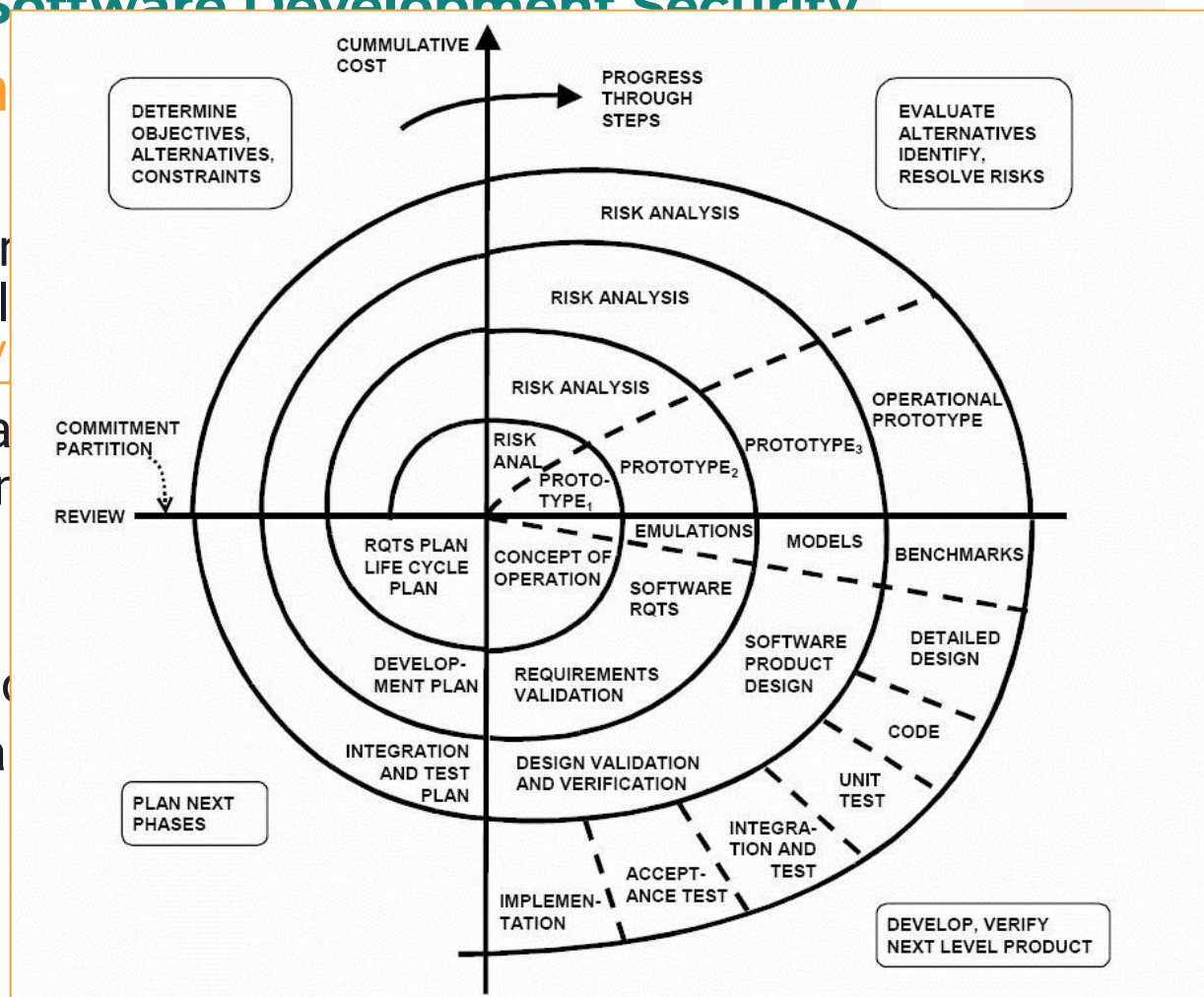
- repeated expansion

- each

- each

- method

- risk a





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- **Agile Software Development**
  - Agile Software Development evolved as a reaction to rigid software development models such as the Waterfall Model. Agile methods include **Scrum** and **Extreme Programming (XP)**.
- The Agile Manifesto (See: <http://agilemanifesto.org/>) states: “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”





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- **Scrum**

- named after a scrum in the sport of rugby
- contain small teams of developers, called the Scrum Team
- supported by a Scrum Master, a senior member of the organization who acts like a coach for the team
- the Product Owner is the voice of the business unit



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- **Extreme Programming (XP)**
  - pairs of programmers who work off a detailed specification
  - high level of customer involvement
  - XP core practices include:
    - 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.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- **Rapid Application Development (RAD)**
  - Rapid Application Development (RAD) rapidly develops software via the use of prototypes, “dummy” GUIs, back-end databases, and more.
  - The goal of RAD is quickly meeting the business need of the system;
  - Technical concerns are secondary.
  - The customer is heavily involved in the process.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Application Development Methods

- **Prototyping**

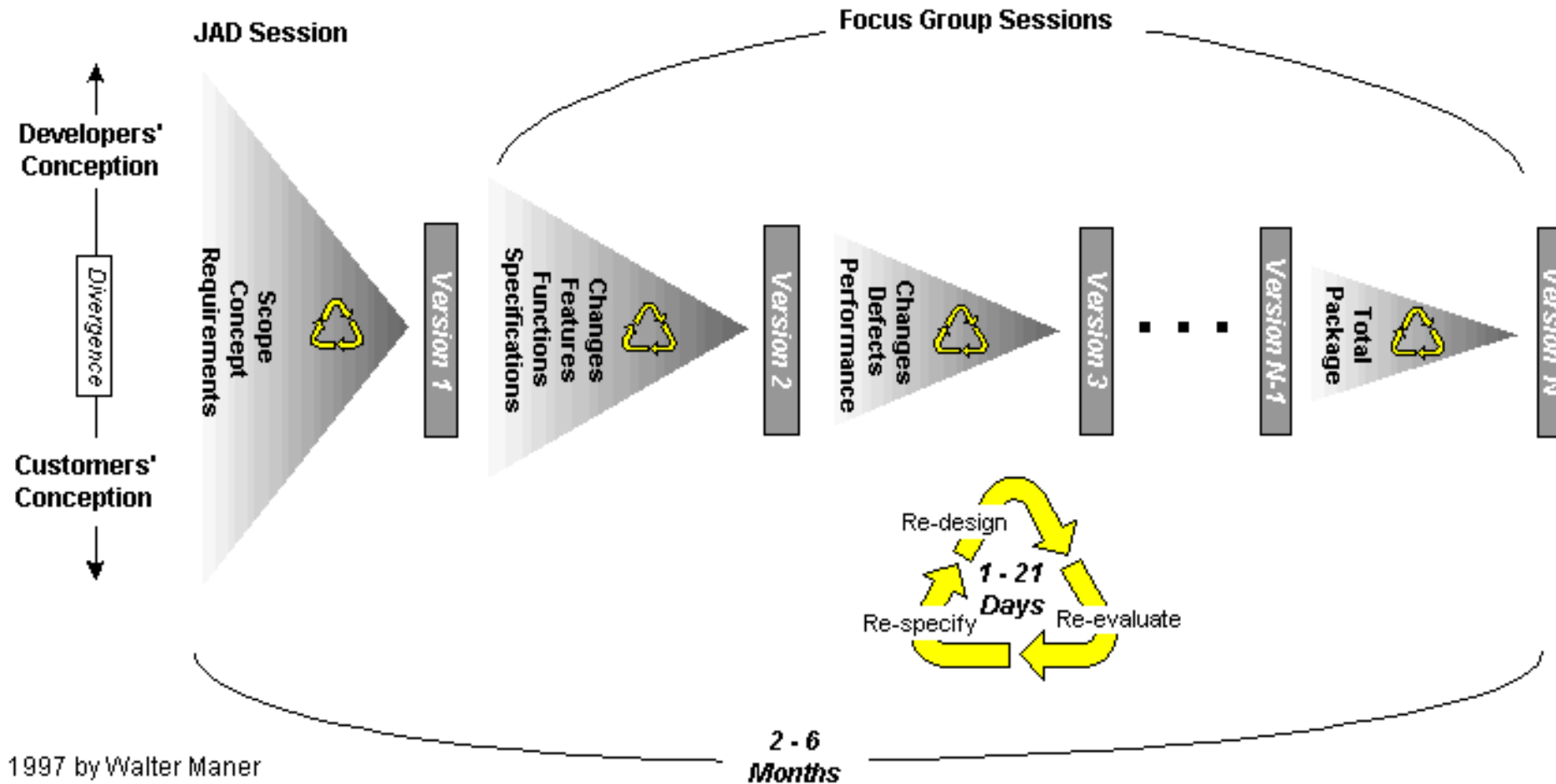
- Prototyping is an iterative approach which breaks projects into smaller tasks, creating multiple mockups (prototypes) of system design features.
- Lowers risk by allowing the customer to see realistic-looking results long before the final product is completed.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

## LECTURE

## RAPID APPLICATION DEVELOPMENT USING ITERATIVE PROTOTYPING





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Systems Development Life Cycle

- (SDLC, also called the Software Development Life Cycle or simply the System Life Cycle)
- On the exam, SDLC focuses on security in every phase
- Broader than many application development models, focusing on the entire system, from selection/development, through operational requirements, to secure disposal.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Systems Development Life Cycle

- The following overview is summarized from NIST SP 800-14:
  - **Operation/Maintenance:** The system is modified by the addition of hardware and software and by other events.
  - **Disposal:** The secure decommission of a system.

In actuality, NIST SP 800-14 has been “withdrawn in it’s entirety”.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Systems Development Life Cycle

- Not testable, but I like the OWASP Secure Software Development Lifecycle Project(S-SDLC)
- OWASP Secure Software Development Life Cycle Project defines security software development process.
- Get it here:  
[https://www.owasp.org/index.php/OWASP\\_Secure\\_Software\\_Development\\_Lifecycle\\_Project](https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project)

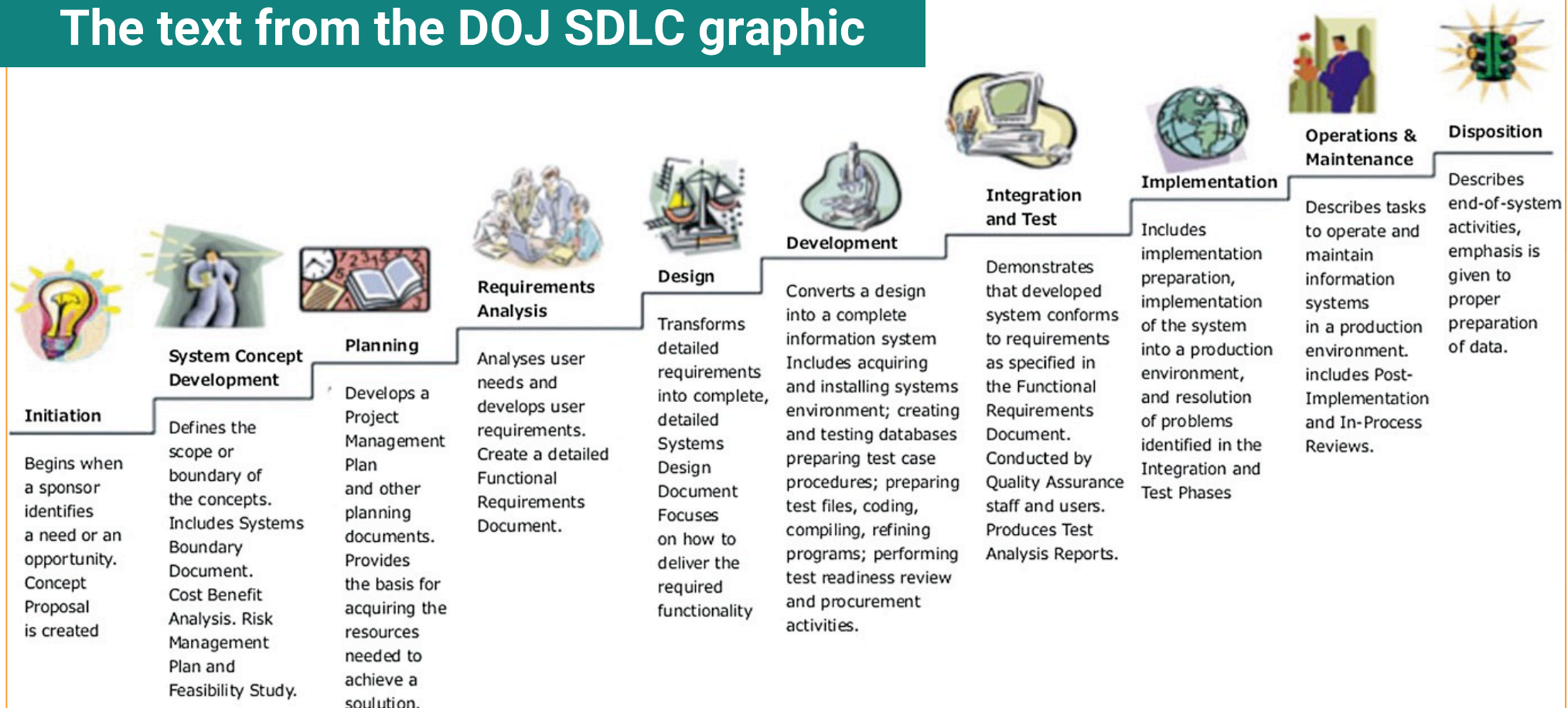




## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# Systems Development Life Cycle (SDLC) Life-Cycle Phases

### The text from the DOJ SDLC graphic





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Escrow

- Software escrow describes the process of having a third party store an archive or computer software.
- The vendor may wish to keep the software source code secret, but the customer may be concerned that the vendor could go out of business (potentially orphaning the software).
- Orphaned software with no available source code will not receive future improvements or patches.
- Software escrow places the source code in escrow, under the control of a neutral third party.
- A contract strictly specifies the conditions for potential release of the source code to the customer, typically due to the business failure of the software vendor.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Code Repository Security

- Public third party code repositories such as GitHub (<http://www.github.com>)
- Accidentally publishing private code as public is a common mistake made by developers. This includes accidentally publishing code that includes passwords or private keys.
- List of security controls:
  - System Security
  - Operational Security
  - Software Security
  - Secure Communications
  - File system and backups
  - Employee access
  - Maintaining security
  - Credit card safety

Really good story on page 448 of the book.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Security of Application Programming Interfaces (APIs)

- An Application Programming Interface (API) allows an application to communicate with another application, or an operating system, database, network, etc.
- OWASP API Security Project  
([https://www.owasp.org/index.php/OWASP\\_API\\_Security\\_Project](https://www.owasp.org/index.php/OWASP_API_Security_Project))
  - “This project is designed to address the ever-increasing number of organizations that are deploying potentially sensitive APIs as part of their software offerings. These APIs are used for internal tasks and to interface with third parties. Unfortunately, many APIs do not undergo the rigorous security testing that would render them secure from attack. ”
- Problems with the security of API servers are notorious.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Change and Configuration Management

- The exam treats configuration management and change management as separate (but related) disciplines
  - Configuration management tracks changes to a specific piece of software
  - Change management is broader, tracking changes across an entire software development program



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Change and Configuration Management

- NIST Special Publication 80-128: Guide for Security-Focused Configuration Management of Information Systems (<http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf>)
- A Configuration Management Plan (CM Plan) is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. The basic parts of a CM Plan include:
  - **Configuration Control Board (CCB)** – Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; may also be referred to as a change control board;
  - **Configuration Item Identification** – methodology for selecting and naming configuration items that need to be placed under CM;
  - **Configuration Change Control** – process for managing updates to the baseline configurations for the configuration items; and
  - **Configuration Monitoring** – process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under CM”



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### DevOps

- Separation of duties between the developers, quality assurance teams, and production teams
- “the practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support.”



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Object-oriented Design and Programming

- Object oriented design and programming uses an object metaphor to design and write computer programs.
- Object-Oriented Programming (OOP) replicates the use of objects in computer programs.
- Object-Oriented Design (OOD) treats objects as a higher level design concept, like a flow chart.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Object-Oriented Programming (OOP)

- Treats a program as a series of connected objects that communicate via messages.
- Attempts to model the real world
- Examples of OOP languages include Java, C++, Smalltalk, and Ruby.
- An object is a “black box” that is able to perform functions, and sends and receives messages.
- Objects contain data and methods (the functions they perform).
- The object provides encapsulation (also called data hiding): we do not know, from the outside, how the object performs its function.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Cornerstone Object-Oriented Programming Concepts

- Cornerstone object-oriented programming concepts include **objects**, **methods**, **messages**, **inheritance**, **delegation**, **polymorphism**, and **polyinstantiation**.
  - **Inheritance** is a way to reuse code of existing objects, establish a subtype from an existing object
  - **Delegation** refers to one object relying upon another to provide a specified set of functionalities
  - **Polymorphism** is the ability to create a variable, a function, or an object that has more than one form
  - **Polyinstantiation** means “many instances,” two instances (specific objects) with the same names that contain different data.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

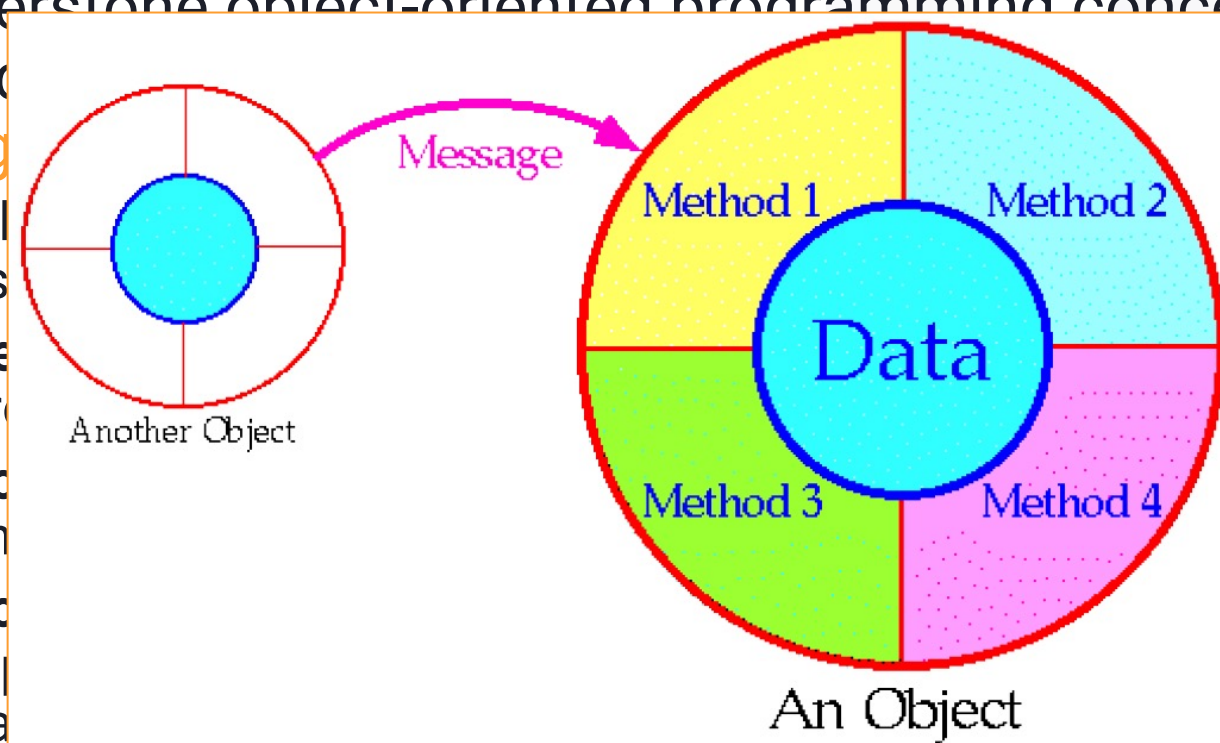
## Domain #8: Software Development Security

### Cornerstone Object-Oriented Programming Concepts

- Cornerstone object-oriented programming concepts

include  
delegation

- Includes
- Delegation
- Polymorphism
- Encapsulation
- Abstraction



tion, or

ces  
fferent



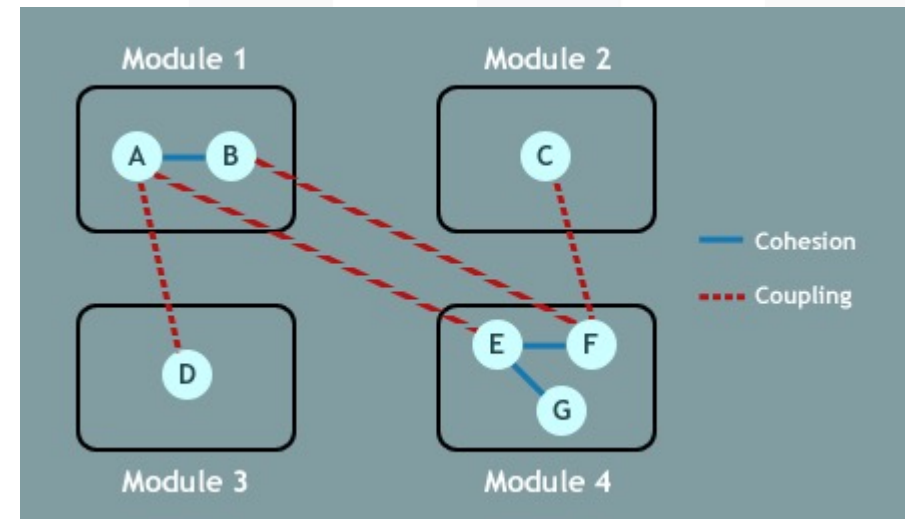
## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Coupling and Cohesion

- Coupling and cohesion are two concepts used to describe objects.
  - A highly coupled object requires lots of other objects to perform basic jobs, like math.
  - An object with high cohesion is far more independent: it can perform most functions independently.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Object Request Brokers

- Object Request Brokers (ORBs) can be used to locate objects: they act as object search engines.
- ORBs are middleware: they connect programs to programs.
- Common object brokers included COM, DCOM, and CORBA.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

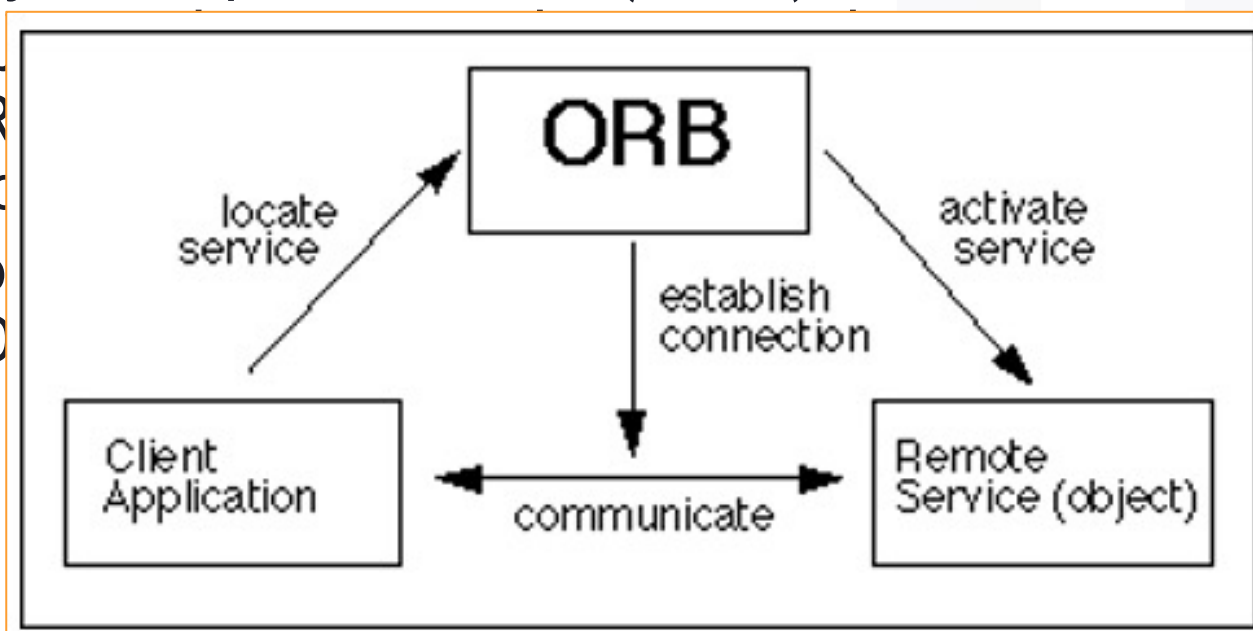
# LECTURE

## Domain #8: Software Development Security

### Object Request Brokers

- Object Request Brokers (ORBs) can be used to locate

- ob
- OR
- pro
- Co
- CO





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### CORBA

- Common Object Request Broker Architecture (CORBA) is an open vendor-neutral networked object broker framework by the Object Management Group (OMG).
- Competes with Microsoft's proprietary DCOM.
- Objects communicate via a message interface, described by the Interface Definition Language (IDL). See <http://www.corba.org> for more information about CORBA.
- The essence of CORBA, beyond being a networked object broker, is the separation of the interface (syntax for communicating with an object) from the instance (the specific object):

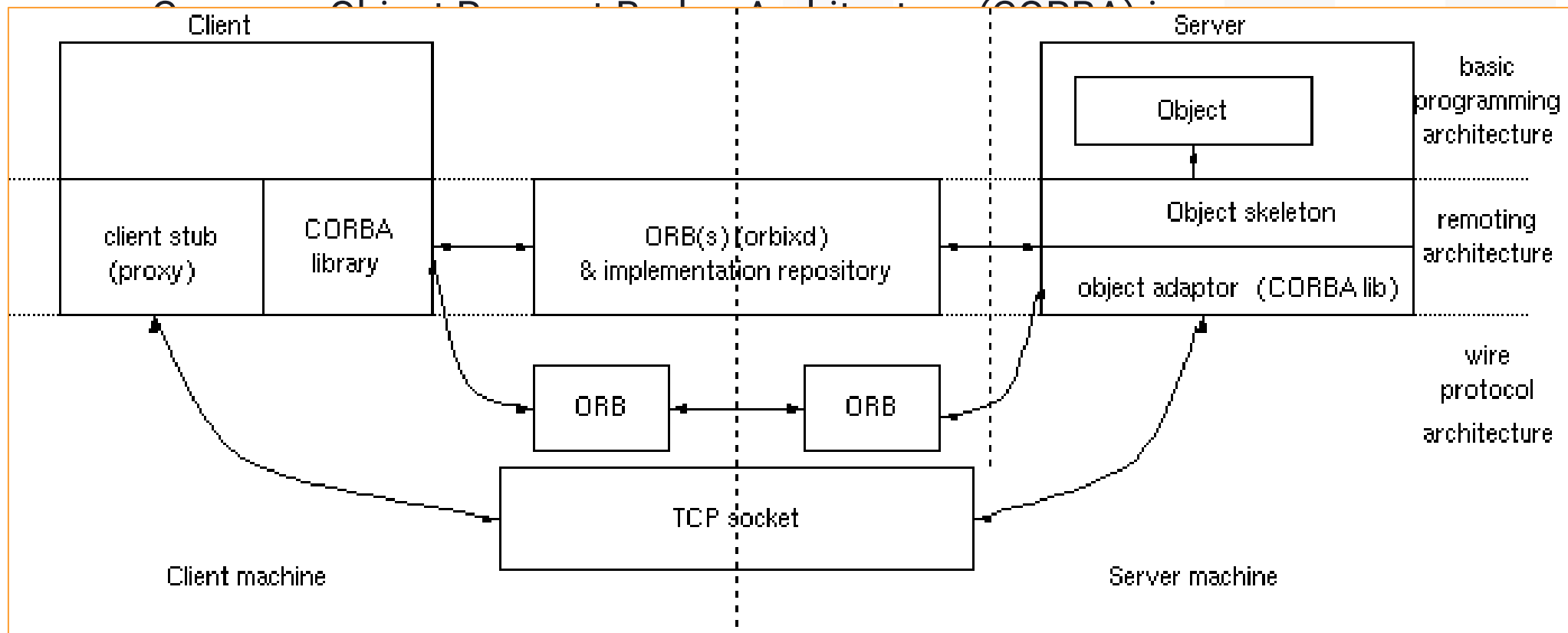


## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### CORBA







## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Object-Oriented Analysis (OOA) and Object-Oriented Design (OOD)

- Object-Oriented Analysis (OOA) and Object-Oriented Design (OOD) are a software design methodology that takes the concept of objects to a higher, more conceptual, level than OOP. The two terms are sometimes combined as Object-Oriented Analysis and Design (OOAD).
- It is like drawing a flowchart on a whiteboard which shows how a program should conceptually operate.
- The way data in a program flows and is manipulated is visualized as a series of messages and objects. Once the software design is complete, the code may be programmed in an OOP language such as Ruby.
- Object-Oriented Analysis (OOA) seeks to understand (analyze) a problem domain (the challenge you are trying to address) and identifies all objects and their interaction. Object-Oriented Design (OOD) then develops (designs) the solution.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Vulnerabilities, Testing, and Assurance

#### Software Vulnerabilities

- 2011 CWE/SANS Top 25 Most Dangerous Software Errors - <http://cwe.mitre.org/top25/>
  - **Hard-coded credentials:** Backdoor username/passwords left by programmers in production code
  - **Buffer Overflow:** Occurs when a programmer does not perform variable bounds checking
  - **SQL Injection:** manipulation of a back-end SQL server via a front-end web server
  - **Directory Path Traversal:** escaping from the root of a web server (such as /var/www) into the regular file system by referencing directories such as “../..”



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Vulnerabilities, Testing, and Assurance

#### TOCTOU/Race Conditions

- attacker attempts to alter a condition after it has been checked by the operating system, but before it is used



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Vulnerabilities, Testing, and Assurance

#### TOCTOU/Race Conditions

- EXAMPLE:

Pseudo-code for a setuid root program (runs with super user privileges, regardless of the running user) called “open test file” that contains a race condition:

1. If the file “test” is readable by the user
2. Then open the file “test”
3. Else print “Error: cannot open file.”

The race condition occurs between steps 1 and 2. Other processes are running while our “open test file” program is running. The computer may run our program like this:

1. If the file “test” is readable by the user
2. Run another process
3. Run another process
4. Then open the file “test”



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Vulnerabilities, Testing, and Assurance

#### Disclosure

- Disclosure describes the actions taken by a security researcher after discovering a software vulnerability.
- **Full Disclosure** is the controversial practice of releasing vulnerability details publicly. The rationale is this: if the bad guys may already have the information, then everyone should also have it. This ensures the white hats also receive the information, and will also pressure the vendor to patch the vulnerability.
- Advocates argue that vulnerable software should be fixed as quickly as possible; relying on (perceived) lack of knowledge of the vulnerability amounts to “Security through obscurity,” which many argue is ineffective. The Full Disclosure mailing list (see: <http://seclists.org/fulldisclosure/>) is dedicated to the practice of full disclosure.
- **Responsible disclosure** is the practice of privately sharing vulnerability information with a vendor, and withholding public release until a patch is available.
- Other options exist between full and responsible disclosure



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Software Vulnerabilities, Testing, and Assurance Databases

- A database is a structured collection of related data.

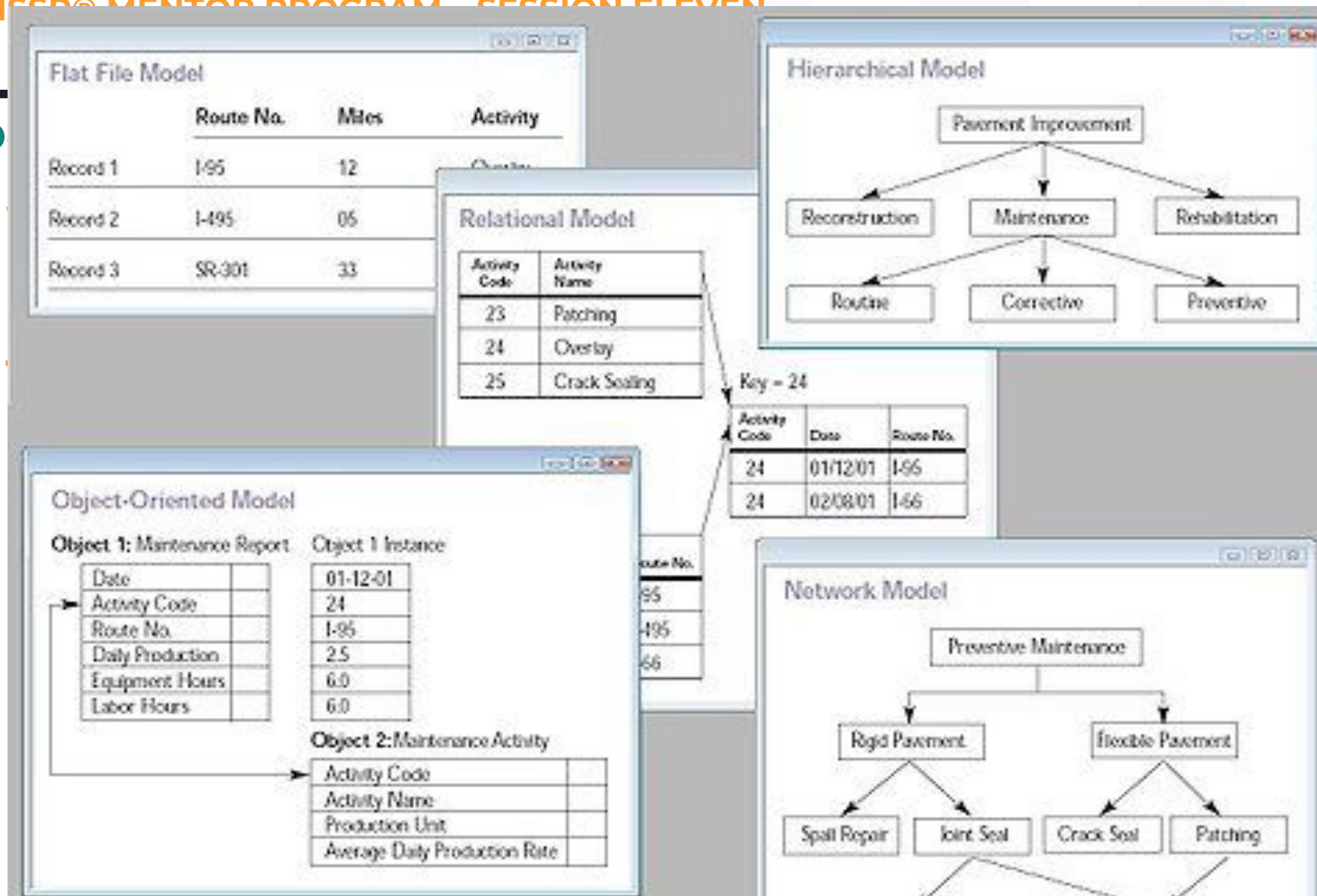
### Types of Databases

- Formal database types include relational (two dimensional), hierarchical, and object-oriented. The simplest form of database is a flat file: a text file that contains multiple lines of data, each in a standard format.



# CISSP® MENTOR PROGRAM SESSION ELEVEN

L  
D





# LECTURE

## Domain #8: Software Development Security

### Relational Databases

- The most common modern database is the relational database, which contain two-dimensional tables of related (hence the term “relational”) data.
- A table is also called a relation.
- Tables have rows and columns: a row is a database record, called a tuple; a column is called an attribute.
- A single cell (intersection of a row and column) in a database is called a value.
- Relational databases require a unique value called the **primary key** in each tuple in a table.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Relational Databases

- A relational database employee table, sorted by the primary key (SSN, or Social Security Number).
- Attributes are SSN, Name, and Title.
- Tuples include each row: 133-73-1337, 343-53-4334, etc. “Gaff” is an example of a value (cell).
- Candidate keys are any attribute (column) in the table with unique values: candidate keys in the previous table include SSN and Name; SSN was selected as the primary key because it is truly unique (two employees could have the same name, but not the same SSN).
- Two tables in a relational database may be joined by the primary key.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Relational Databases

- A relational database employee table, sorted by the primary key (SSN, or Social Security Number).

SSN	Name	Title
133-73-1337	J.F. Sebastian	Designer
343-53-4334	Eldon Tyrell	Doctor
425-22-8422	Gaff	Detective
737-54-2268	Rick Deckard	Detective
990-69-4771	Hannibal Chew	Engineer

- Two tables in a relational database may be joined by the primary key.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Foreign Key

- A foreign key is a key in a related database table that matches a primary key in the parent database.

### Referential, Semantic, and Entity Integrity

- **Referential integrity** means that every foreign key in a secondary table matches a primary key in the parent table.
- **Semantic integrity** means that each attribute (column) value is consistent with the attribute data type.
- **Entity integrity** means each tuple has a unique primary key that is not null.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Database Normalization

- Seeks to make the data in a database table logically concise, organized, and consistent.
- Removes redundant data, and improves the integrity and availability of the database.
- Normalization has three rules, called forms:
  - 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.
  - Third normal Form (3NF): Remove data that is not dependent on the primary key.

### Database Views

- Database tables may be queried; the results of a query are called a database view.
- Views may be used to provide a constrained user interface.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### The Data Dictionary

- The data dictionary contains a description of the database tables.
- This is called metadata: data about data.
- Contains database view information, information about authorized database administrator, and user accounts including their names and privileges, auditing information, among others.
- A critical data dictionary component is the database schema: it describes the attributes and values of the database tables.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Database Query Languages

- Allow the creation of database tables, read/write access to those tables, and many other functions.
- Database query languages have at least two subsets of commands:
  - Data Definition Language (DDL) - DDL is used to create, modify, and delete tables.
  - Data Manipulation Language (DML) - DML is use to query and update data stored in the tables.
- The most popular relational database query language is SQL (Structured Query Language)
  - Created by IBM in 1974
  - Many types of SQL exist, including MySQL, PostgreSQL, PL/SQL (Procedural Language/SQL, used by Oracle), T-SQL and ANSI SQL (used by Microsoft SQL), and many others.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Database Query Languages

- 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



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Hierarchical Databases

- Hierarchical databases form a tree: the global Domain Name Service (DNS) servers form a global tree.

### Object-oriented Databases

- Databases traditionally contain just (passive) data; object-oriented databases combine data with functions (code) in an object-oriented framework.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Database Replication and Shadowing

- Database replication mirrors a live database, allowing simultaneous reads and writes to multiple replicated databases by clients.
- Shadow databases are similar to replicated databases, with one key difference: a shadow database mirrors all changes made to a primary database, but clients do not access the shadow.

### Data Warehousing and Data Mining

- A data warehouse is a large collection of data. Modern data warehouses may store many terabytes (1000 gigabytes) or even petabytes (1000 terabytes) of data.
- Once data is collected in a warehouse, data mining is used to search for patterns.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Artificial Intelligence

- Artificial Intelligence is the science of programming electronic computers to “think” more intelligently, sometimes mimicking the ability of mammal brains.

### Expert Systems

- Expert systems consist of two main components:
  - The first is a **knowledge base** that consists of “if/then” statements. These statements contain rules that the expert system uses to make decisions.
  - The second component is an **inference engine** that follows the tree formed by the knowledge base, and fires a rule when there is a match.
- Integrity of the knowledge base is critical.
- The entire knowledge base should form a logical tree, beginning with a trunk. The knowledge base should then branch out.
- The inference engine follows the tree, branching or firing as if/then statements are answered.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Artificial Neural Networks

- Simulate neural networks found in humans and animals.
- The human brain's neural network has 100 billion neurons, interconnected by thousands or more synapses each.
- Each neuron may fire based on synaptic input.
- This multilayer neural network is capable of making a single decision based on thousands or more inputs.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Artificial Neural Networks

- How Artificial Neural Networks Operate
  - ANNs seek to replicate the capabilities of biological neural networks.
  - A node is used to describe an artificial neuron.
  - Nodes receive input from synapses and send output when a weight is exceeded.
  - Single-layer ANNs have one layer of input nodes; multilayer ANNs have multiple layers of nodes, including hidden nodes
  - Both single and multilayer artificial neural networks eventually trigger an output node to fire: this output node makes the decision.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Artificial Neural Networks

- An Artificial Neural Network learns by example via a training function: synaptic weights are changed via an iterative process, until the output node fires correctly for a given set of inputs.
- Artificial Neural Networks are used for “fuzzy” solutions, where exactness is not always required (or possible), such as predicting the weather.



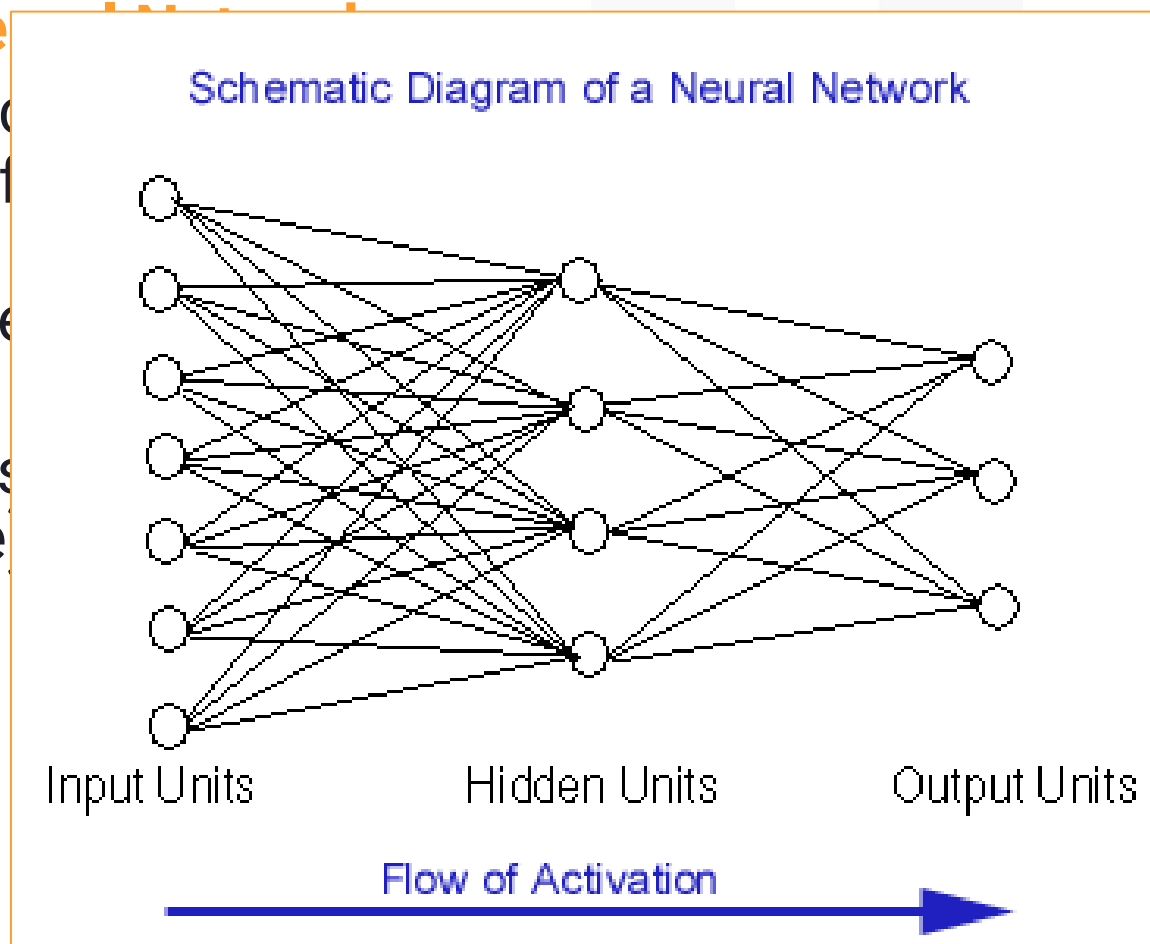
## CISSP® MENTOR PROGRAM – SESSION ELEVEN

## LECTURE

## Domain #8: Software Development Security

## Artificial Neural Networks

- An Artificial Neural Network is a training process that is iterative for a given set of data.
- Artificial Neural Networks can find solutions that are not possible for a human.



a  
a an  
ctly

(or



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Bayesian Filtering

- Bayesian filtering is named after Thomas Bayes, an English clergyman who devised a number of probability and statistical methods including “a simple mathematical formula used for calculating conditional probabilities.”
- Commonly used to identify spam.
- Bayesian filtering techniques to automatically assign a mathematical probability that certain “tokens” (words in the email) were indications of spam.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Genetic Algorithms and Programming

- Genetic Algorithms and Programming seek to replicate nature's evolution, where animals evolve to solve problems.
- Genetic programming refers to creating entire software programs (usually in the form of Lisp source code)
- Genetic algorithms refer to creating shorter pieces of code (represented as strings called chromosomes).
- Genetic programming creates random programs and assigns them a task of solving a problem.
- The fitness function describes how well they perform their task.
- Crossover “breeds” two programs together (swaps their code).
- Mutation introduces random changes in some programs.





## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Genetic Algorithms and Programming

- The process is summarized here:
  - 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)
- Genetic Algorithms and Genetic Programming have been used to program a Pac-Man playing program, robotic soccer teams, networked intrusion detection systems, and many others.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

# LECTURE

## Domain #8: Software Development Security

### Genetic Algorithms and Programming

- The process is summarized here:
  - 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)
- Genetic Algorithms and Genetic Programming have been used to program a Pac-Man playing program, robotic soccer teams, networked intrusion detection systems, and many others.



## CISSP® MENTOR PROGRAM – SESSION ELEVEN

**LECTURE**

## Domain #8: Software Development Security

# We made it through Class 11!

## This concludes all of the content for the CISSP

- We're done with the book.
- Next, we do practice exams. YOU need to read, read, read (and memorize).
- Come with questions!

Have a great evening, talk to you Wednesday!