national center for ontological research
ncor

University at Buffalo
The State University of New York

Design Patterns: Practice

John Beverley

Assistant Professor, *University at Buffalo*
Co-Director, National Center for Ontological Research
Affiliate Faculty, *Institute of Artificial Intelligence and Data Science*

Outline

- Lists of Entities

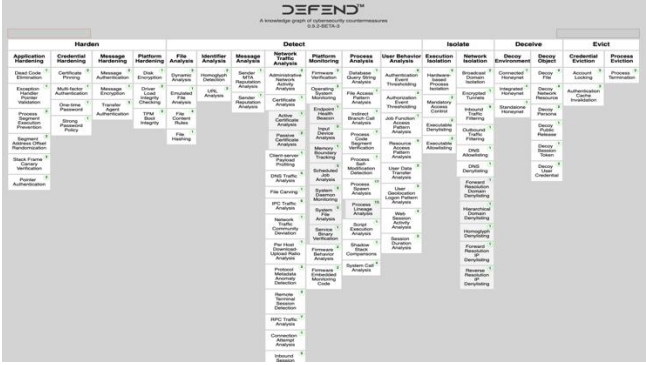
- Design Pattern

Outline

- Lists of Entities

- Design Pattern

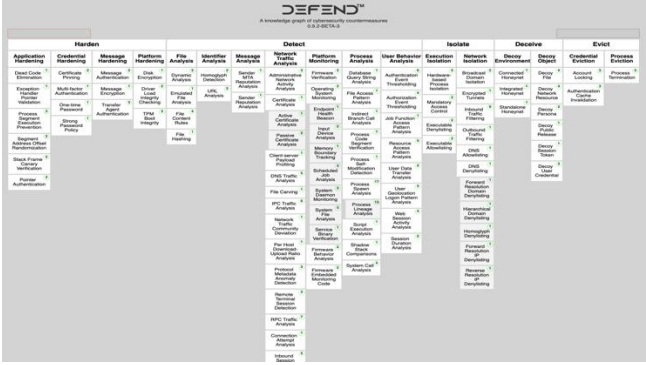
Competency Question



SELECT AND MODEL THE FOLLOWING

Information is encrypted on a solid-state drive.

Competency Question



SELECT AND MODEL THE FOLLOWING

Information is encrypted on a solid-state drive.

List:

- **Material entities involved in the encryption of a hard drive**
- **Qualities of those material entities**
- **Processes they participate in**
- **Information borne by the material entities**

Here are four lists for the design pattern involving encryption on a solid-state drive:

1. Material Entities Involved
- **Solid-State Drive (SSD)**: The main storage medium.
- **Encryption Module**: Hardware or software component managing the encryption.
- **Controller Chip**: Manages data flow and encryption/decryption processes.
- **Data Bus**: Transfers data between the SSD and other components.
- **Random Access Memory (RAM)**: Temporary data storage for processing.
- **Key Storage Module**: Securely stores cryptographic keys used in encryption.

2. Qualities of These Material Entities
- **Storage Capacity** (SSD): Determines data volume that can be encrypted.
- **Read/Write Speed** (SSD): Impacts performance during encryption processes.
- **Security Level** (Encryption Module): Indicates robustness of encryption standards.
- **Data Transfer Rate** (Data Bus): Speed of data transmission affects encryption efficiency.
- **Reliability** (Key Storage): Stability and integrity in storing encryption keys.
- **Power Efficiency** (Controller Chip): Determines power consumption during encryption.

3. Processes They Participate In
- **Data Encryption**: Converting data into a secure format.
- **Data Decryption**: Reverting encrypted data to its original format.
- **Key Generation**: Creating secure keys for encryption.
- **Key Management**: Storing, retrieving, and managing encryption keys.
- **Data Transfer**: Moving data to and from the SSD.
- **Data Integrity Check**: Verifying that data remains unaltered post-encryption.

4. Information Borne by the Material Entities
- **Encrypted Data**: The actual information in encrypted form on the SSD.
- **Encryption Keys**: Unique codes that allow data to be encrypted or decrypted.
- **Access Logs**: Records of encryption and decryption events for security tracking.
- **Encryption Metadata**: Details about encryption algorithms and parameters used.
- **User Authentication Data**: Credentials needed for accessing encrypted data.
- **Error Codes**: Information on any issues encountered during encryption/decryption.

These lists illustrate the interactions and attributes relevant to an encryption-enabled SSD system.

Information is encrypted on a solid-state drive

- List material entities involved in encryption of a hard drive
  - SSD
  - Computer
  - flash memory cells
- Qualities of those material entities
  - Storage Capacity
- Processes they participate in
  - Encrypting
  - Storing
  - Accessing
- Information borne by the material entities

SSD ~ internal SSD
external SSD
flash memory

Computer

Speed
Durability
Reliability
~~Energy~~ Energy Efficiency
Noise + Heat (heat resistence)
Size (compact)
cost
Capacity
Encryption
Wear leveling
Shape

-Material Entity

- Hard Drive - Flash memory
- SSD
- Computer ex
- Wire connection

Quality

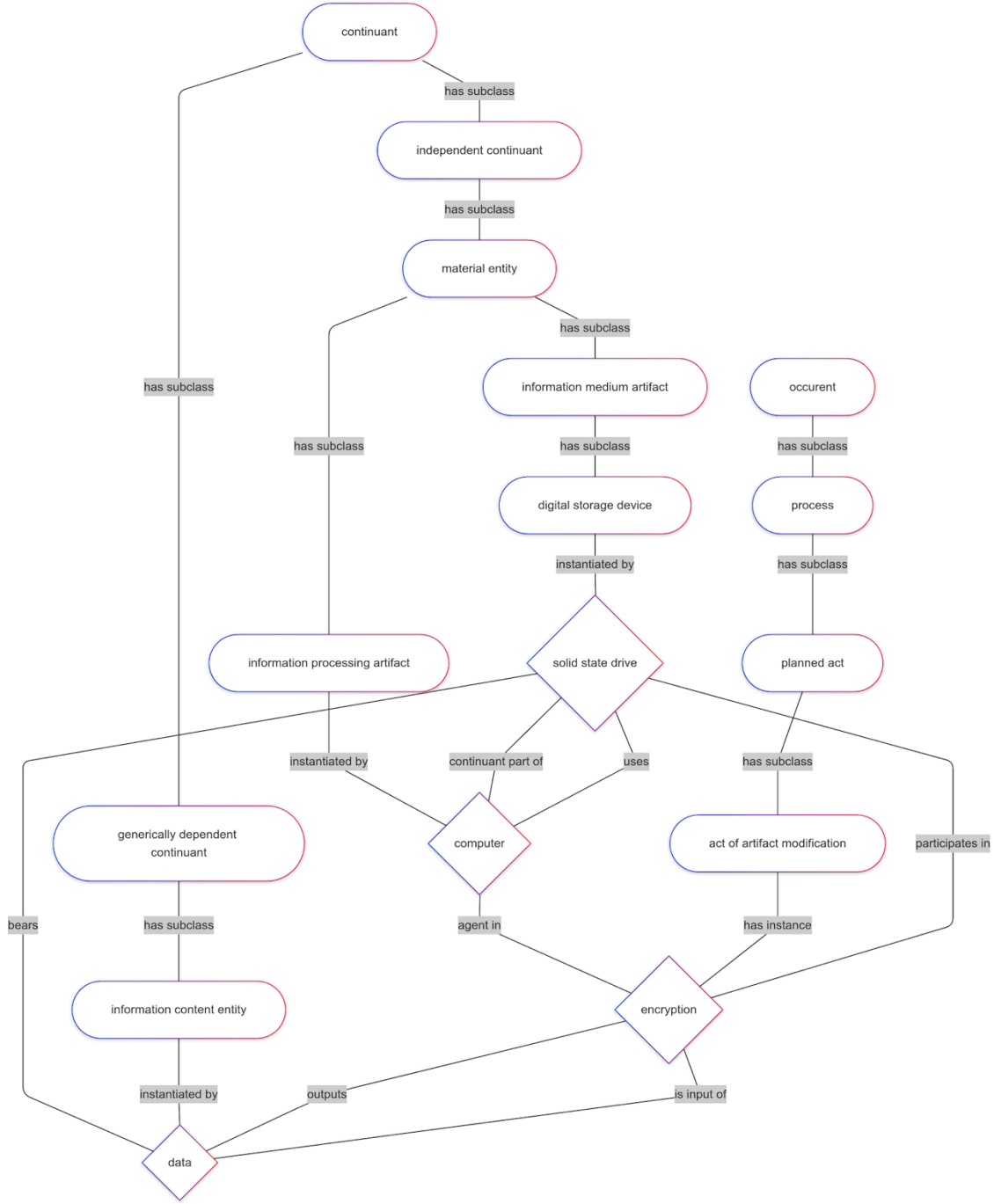
- Store (blocks)

Process

- Storage
- Encryption (information)
- Data Representation
- Access Control
- Decryption

Info Born

- Encrypted Data/ Cipher Text
- Access Info/ Identity Info (passphrase)

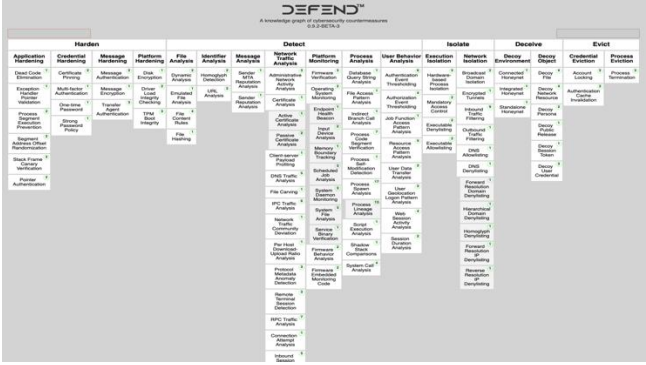

continuant
has subclass
independent continuant
has subclass
material entity
has subclass
has subclass
information medium artifact
occurent
has subclass
has subclass
has subclass
digital storage device
process
instantiated by
has subclass
information processing artifact
solid state drive
planned act
instantiated by
continuant part of
uses
has subclass
generically dependent continuant
computer
act of artifact modification
participates in
bears
has subclass
agent in
has instance
information content entity
encryption
instantiated by
outputs
is input of
data

Outline

- Lists of Entities

- Design Pattern

Competency Question



SELECT AND MODEL THE FOLLOWING

Information is encrypted on a solid-state drive.

Guidance Part 1

- Your group should have a different composition this meeting than in the previous meeting where we discussed design patterns

- Select a design pattern list to discuss and evaluate it in the following way:

  - A person who was part of the team that created it, will summarize the decisions
  - Others will listen without comment
  - Next the group will consider whether anything is missing or unnecessary

Guidance Part 2

- Review the list of entities you created and place them, if you have not, under their appropriate parent classes in BFO/CCO

- Diagram this with ovals, diamonds, etc.

- Next, connect entities by appropriate relations, using arrows in the graph

Guidance Part 3

- You should expect this to be an iterative process; you should expect to make some mistakes

- Once you have created a handful of relationships among entities, you will then organize yourselves into:

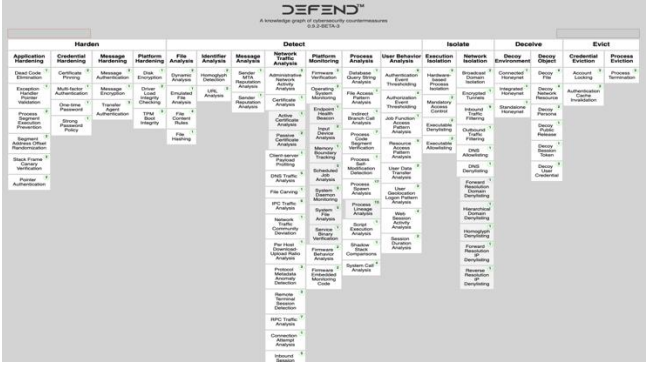
Guidance Part 3

- You should expect this to be an iterative process; you should expect to make some mistakes

- Once you have created a handful of relationships among entities, you will then organize yourselves into:

Dogmatist
Academic
Skeptic

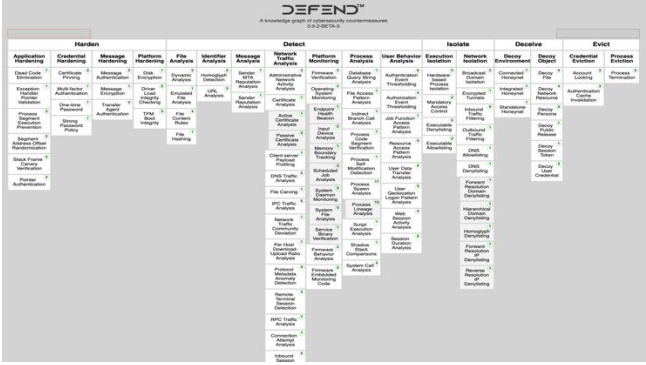
Competency Question



SELECT AND MODEL THE FOLLOWING

Information is encrypted on a solid-state drive.

Competency Question

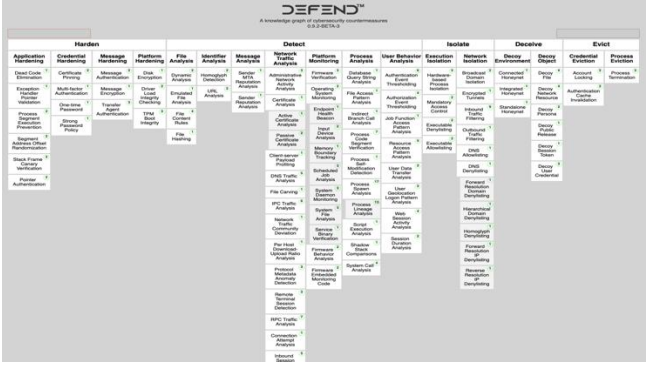


SELECT AND MODEL THE FOLLOWING

Information is encrypted on a solid-state drive.

PART 1: SUMMARIZE AND REVIEW

Competency Question

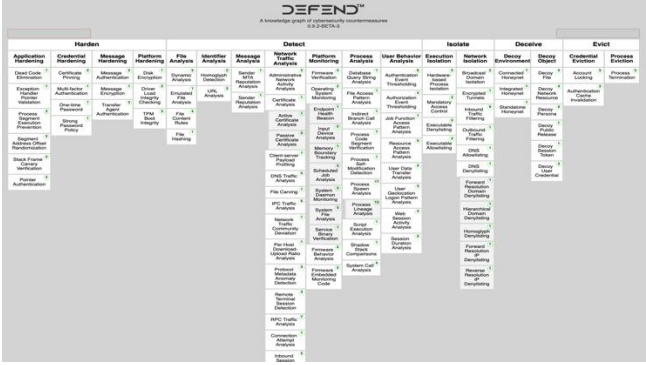


SELECT AND MODEL THE FOLLOWING

Information is encrypted on a solid-state drive.

PART 2: ONTOLOGY PLACEMENT

Competency Question



SELECT AND MODEL THE FOLLOWING

Information is encrypted on a solid-state drive.

PART 3: DOGMATIST, ACADEMIC, SKEPTIC