INDIAN INSTITUTE OF TECHNOLOGY (BHU) VARANASI

Name: Gaurav Kumar **Branch: CSE(IDD)**

Roll Number: 17074008 **Year: Third**

Subject Name: Stream Project(UG) **Subject Code: CSE392**

Instructor Name: Dr. Anil Kumar Tripathi and Dipti Tripathi
aktripathi.cse@iitbhu.ac.in
diptytripathi.rs.cse17@iitbhu.ac.in

DECLARATION OF ORIGINALITY OF WORK

I affirm that the attached project is entirely my own except where the words or ideas of other writers are specifically acknowledged through the use of inverted commas and in-text citations. This assignment has not been submitted for any other subject or other institution. I have revised, edited, and proofread it before submission.

Ontology

Gaurav Kumar
gaurav.kumar.cse17@itbhu.ac.in

Abstract

In the report, there is an attempt to explore from the basics to the roots of ontology and security where you will view history as well as implementation of ontology using rdfs and other techniques.The pre-knowledge from past researhes can be viewed and are referenced.

Introduction to Ontology

Ontology aims to detect the missing security constructs in security requirements modeling frameworks and facilitates their enhancement. It is a special kind of information(computational) object which models the structures of the system in the form of entities and relationship.

Philosophical definition: The study of attributes that belong to things because of their very nature which focuses on nature and structure of things is known as ontology.

A body of formally represented knowledge is based on conceptualisation of the objects, concepts and other entities that are assumed to exist in some area of interest and the relationships that hold among them.

Vurnabilities: It is the weakness in the requirement, design and implentation which attackers exploit to compromise the system.

Analysis should answer three basic questions:
1. How a vurnabilty enters into the system?
2. When it enters into the system?
3. Where it is manifested in the system?

Risk: Risk involves the probability of a successful attack and its severity on the system.

Attack: An attack is a set of intentional unwarranted (malacious) actions designed to compromise confidentiality, integrity, availability or any other desired feature of an IT system.

Countermeasure: A protection mechanism employed to secure the system. It can be action, process, devices, solutions, or systems such as firewalls, protocols, digital sign, etc. The logical attack paths is used to trace all possible attack paths.

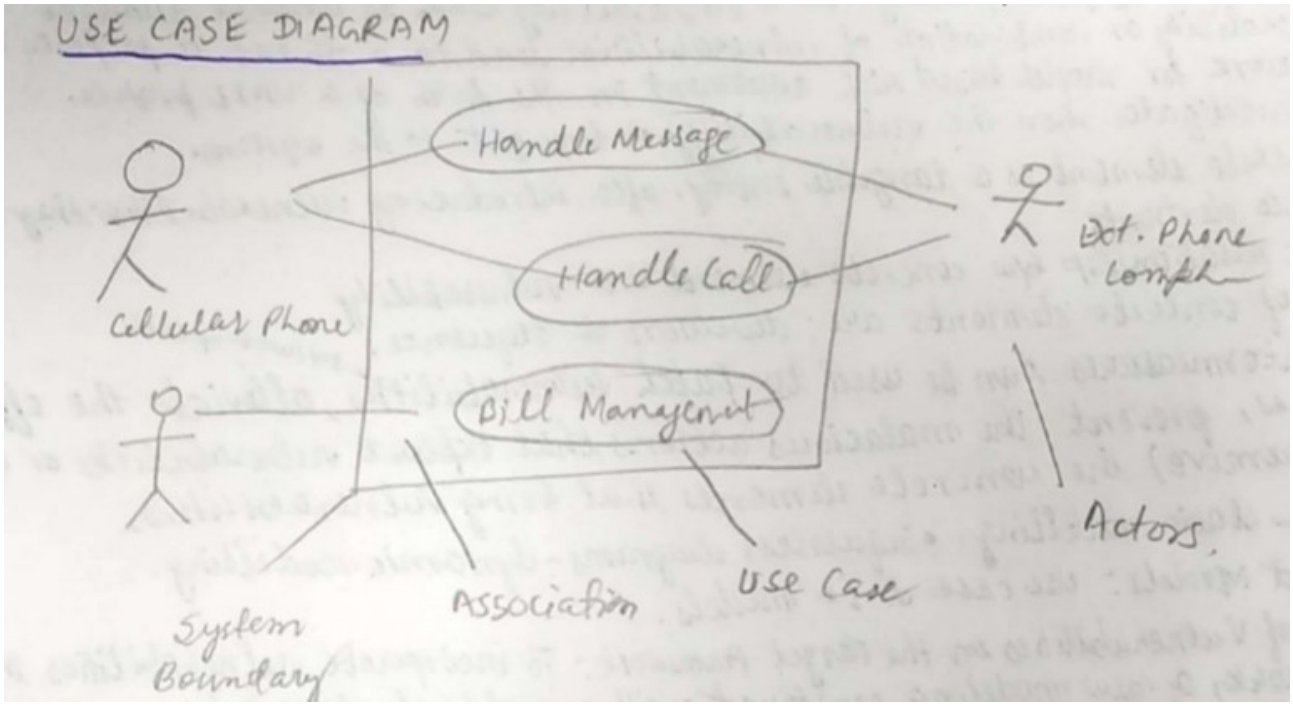
CORAS: Coras provide a way for expressing how a vulnerability leads to another vulnerability or combination of vulnerabilities lead to threat. It proposes a modeling framework for model-based risk assessment in the form of a UML profile.

CORAS doesn't investigate how the vulnerability entered the system. It provides modelling constructs to express threats, vurnabilities, threat scenarios, unwanted incidents, risks, assets and treatement scenarios.

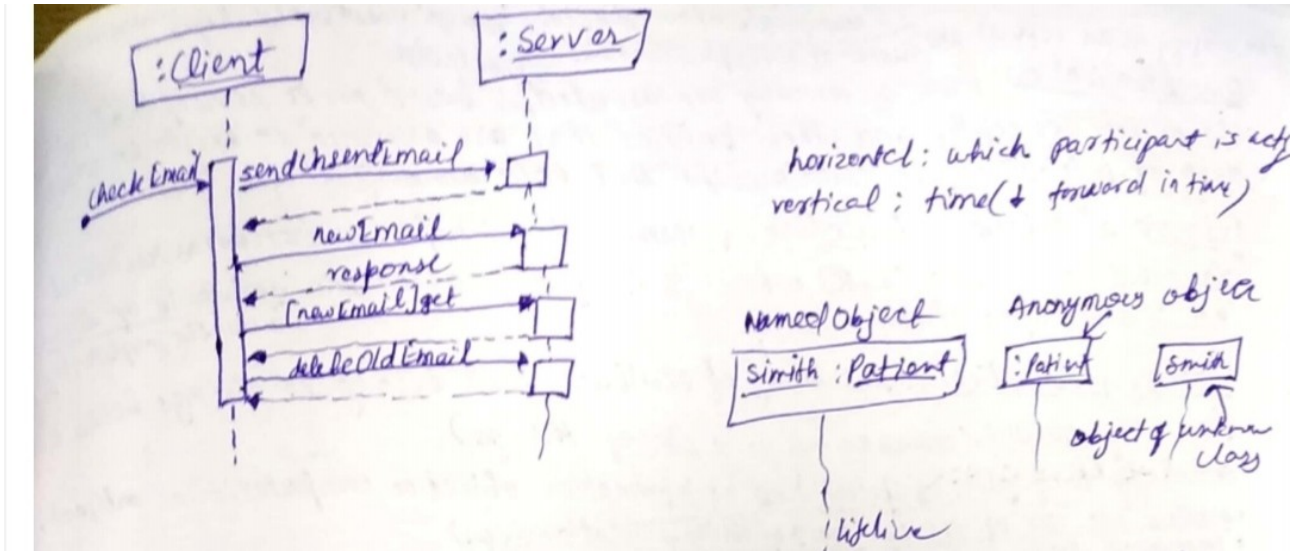
Concrete: A concrete element is a tangible entity, after introducing vulnerable entities they are called vulnerable elements.

Representation and Logical Paths:

Unified Model Language(UML):
UML are pictures of an OO system. Programming languages are not abstract enough for OO design. UML is an open standard and lots of companies use it.
Uses : 1. as a sketch.
2. as a programming language and its applications.
3. as a blueprint.



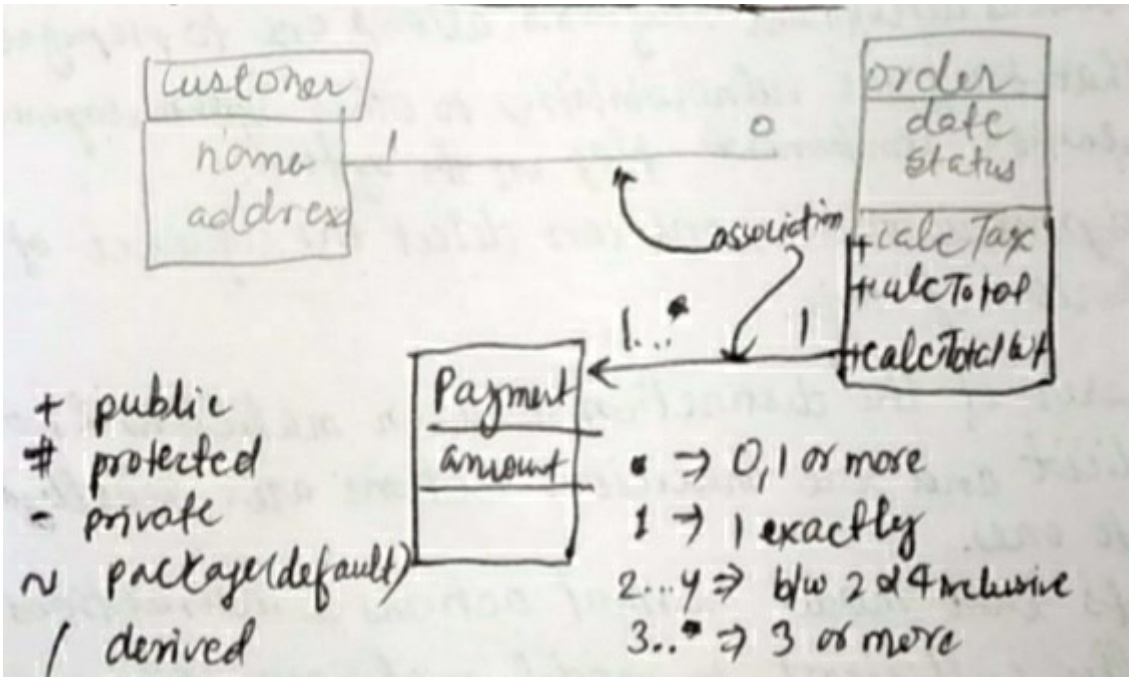
UML Sequence Diagram:
Sequence Diagram is an interaction diagram that models a single scenario executing in a system.



Horizontal: Name of the participant acting.
Vertical: Forward in time in downward direction.

Synchronous message: solid arrow with a solid head.
Asynchronous message: solid arrow with a stick head.

Class Diagram:
Class is represented by solid line and termination by black arrow.
Abstract class is denoted by solid line and white arrow.
Interface shown by dashed line and white arrow.



Some useful notations:

+	public
#	protected
-	private
/	derived
~	package(default)

*****	0,1 or more
1...*	1 or more
2...4	between 2 & 4 inclusive

Conceptualisation:
An ontology is an explicit specification of conceptualisation. A body of formally represented knowledge is based on a conceptualisation: the objects, concepts and other entities that are assumed to exist in some area of interest and the relationships that hold among them.

Extensional Relational Structure: Mathematical representation as relational structure as a tuple (D,R) where D is a set called the universe of discourse. R is a set of relations on D.

Propositional Logic: It is a kind of statement logic (/\,\/ etc and form of complex statements).

Predicate Logic:
1. Unary: Integers, and relationships between unique terms of the set donot exist.
2. Binary: Two terms are defined by particular relationship.
Example: Younger(Sam,Ram).

World: World state for s is a maximum oseervate state of affairs, i.e. a unique assignment of values to all the observable state of affairs.

Intensional(Conceptual) Relation:
An intensional relation of n arity on <D,W> is a total function $\rho^n : W \to 2^{D^n}$ from the set W into the set of all n-ary (extensiional) relations on D.

Where S: arbitrary system
D: arbitrary set of distinguished elements of S.
W: set of world states of S.
<D,W> is domain space for S.

*** Structure:**

C=(D,W,R)

where D: universe of universe
W: set of possible worlds
R: set of conceptual relation on Domain space <D,W>.

R= {Person^1, Manager^1,Reseacher^1, cooperates-with^2}

Reality--------->Perception---------->Conceptualisation
(Phenomena) (Presentations Patterns) (Relevant presentation patterns: D,R)

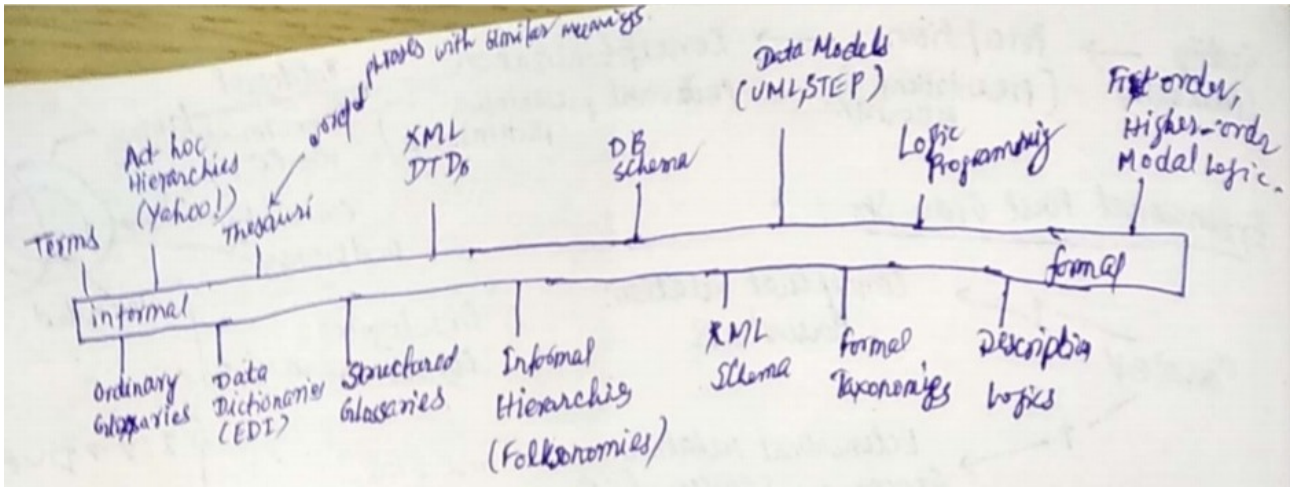
Extensional First Order Structure:

*person ∈ V 1. Conceptual relation: Person^1∈R
2. Extensional Relation: {1000001,....,1050000,...}∈ R

Conceptualisation: C(D,W,R); Vocabulary: V; Model: M = (S,I).

S = (D,R) is an intented model of L according to K if and only if:
1. For all constant symbols C ∈ V we have I(C) = I'(C)
2. There exists a world w∈ W such that, for each predicate symbol v ∈ V there exists an individual relation $\rho \in R$ such that $I(v) = \rho$ and $I(v) = \rho(w)$

* The set $I_k(L)$ of all models of all models of L that are compatible with k is called the set of intended models of L according to K.



Ontology Definition(In terms of set theory**):**
Let C be a conceptualisation, on L a logical language with vocabulary V and ontological commitment K. An ontology Ok for C with vocabulary V and ontological commitment K is a logical theory consisting of a set of formulas of L, designed so that the set of its models approximates as well as possible the set of intended models of L according to K.

Even a perfect ontology like that may fail to exactly specify its target conceptualisation, if its vocabulary and its domain of discourse are not suitably chosen.

Logical motion of model:
A combination of assignments of abstract relational structures (built over the domain of discourse) to vocabulary elements.

Ontological notion of possible worlds is a combination of actual (observed) states of affairs of a certain system. The degree to which an ontology species a conceptualisation depends: 1. On the richness of the domain of discourse 2. On the richness of the vocabulary chosen. 3. On the axiomatization.

First Order Logic:
1. Description Logic: OWL-DL (Web Ontology Logic)
2. Logic Programming: F-Logic (Logic programming selects only a subset of models to judge semantic entailment of formulae**).**

Description Logic

When one wants to complete hierarchy, Description logics (DLs) are a family of knowledge represesntation languages that can be used to represent the knowledge of an application domain in a structured and formally well-understood way. Abox assertions: Happyman(Bob); haschild(Bob,Mary). DL statement must be consistent.

DL has well defined symantics and powerful reasoning tools.

Phase 1: Structural Subsumption Algorithm
First normalise the concept descriptions and then recursively compare the syntactic structure of the normalised descriptions. It is eddicient but they complete for inexpensive Dls. Example: KLONE, K-REP, BACK, LOOM,etc

Phase 2: Tableau Based Algorithm
They work propositionally closed Dls and are complete also for expresssive DLs. It tries to construct a model of it by breaking down the concept in the knowledge base. Example: KRIS, CRACK, etc.

Expansive Description Logic SHIQ
SHIQ allows for rather expressive roles which can be used as definition of concepts:

Definition 1: The set of all SHIQ roles is R U {r- | r ∈ R } where r- is the inverse of role r. Let O be a set of concept names:
1. Every concept name A ∈ C is a SHIQ- concept.
2. If C & D we SHIQ-concept and r is a SHIQ role, then C ∩ D, C U D, ~C, VrC, etc are SHIQ concepts.
3. If C is a SHIQ concept, r is a simple SHIQ role & n ∈ N. Then (<= n r.C) and (>= n r.C) are SHIQ concepts.
Where R-> set of role names; R_+ -> set of transitive roles and R_p -> set of normal roles

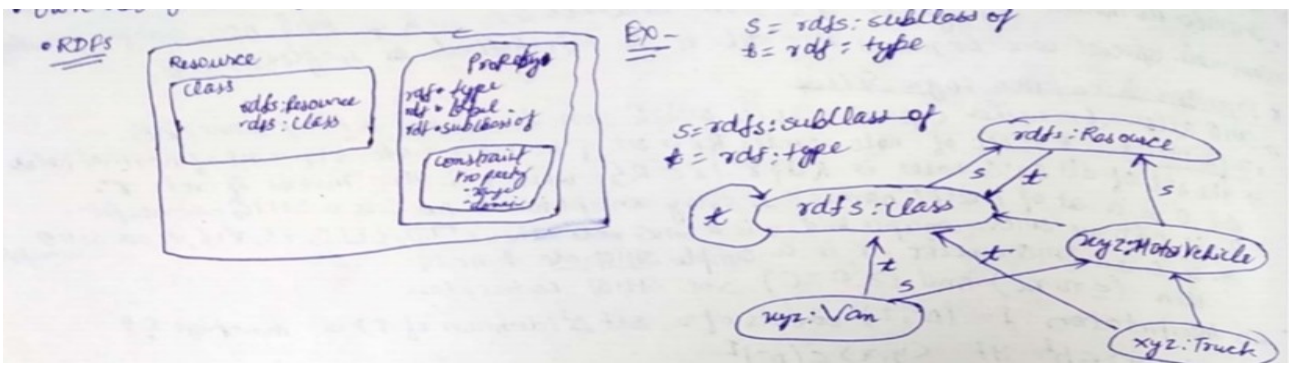
Definition 2: (T Box**):** A role inclusion axiom is of the form r ⊆ S, where r,s are SHIQ roles. A general concept inclusion (GCI) is of the form C ⊆ D where C, D are SHIQ concepts holds for each r ⊆ s ∈ T & C^I ⊆ D^I for each C ⊆ D ⊆ T.

Definition 3: Let I be a set individual names disjoints from R & C. For a,b ∈ I individual names, C a possibly complex SHIQ concept and r a SHIQ role:
* C(a) is called a concept assertion and r(a,b) is a role assertion [A Box].

Definition 4: The concept C is called satifiable with respect to the Tbox T iff there is a model I of T with C^I ≠ Φ. Such an interpretation is called model of C with respect to T.

Desirable features identified for a Web Ontology Language:
1. Compatible with web standards.
2. Easy.
3. Formally.
4. Expressive.

RDFS:
RDF is a data model that provides a way to express simple statements about resources, using named properties and values.



OWL
OWL has great degree of inferencing than RDF schema. It has two types:
1. OWL (SHOIN(D)) (W3C Recommendation since 2004)
2. OWL (SHOIQ(D)) (W3C Recommendation since 2009)
***** Absence of information must not be valued negative information. Eg. sitsNextTo(Person A, Person B) i.e., Person Aalso sits next to B.

OWL1 is based on **SHOIN(D)**.

Axioms:
* TBox : subclass relatioships C ⊆ D
* RBox : subproperty relationships R ⊆ S(H); inverse properties R- (I), transitivity ⊆+ (S)
* ABox : facts for classes C(a), properties R(a,b), equality a=b and difference
* closed classes (nominals) : {a} (0)
* Datatypes (D)

Security System based on Spring jena project has been improved and updated:
https://github.com/grvk28/SpringMVC-Hotel-Reservation-System

References:

1. Handbook on Ontologies by S. Staab and R. Studer

2. https://security1.win.tue.nl/~zannone/publication/elah-yu-zann-09-ER.pdf

3. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6163186/

4. http://cgi.di.uoa.gr/~pms547/lectures/introduction-to-rdf-schema-revised-1spp.pdf

5. http://jena.apache.org/download/

6. https://gitbox.apache.org/repos/asf?p=jena.git

7. http://w3schools.sinsixx.com/rdf/rdf_schema.asp.htm