

## RISK ASSESSMENT IN LAYERED SOLUTIONS

### Commercial Solutions for Classified (CSfC), Risk Analysis

Christopher E. Martinez<sup>1</sup>, *Purdue University*; Robert L. Haverkos<sup>2</sup>, *Purdue University*

<sup>1</sup>Marti606@Purdue.edu, <sup>2</sup>RHaverko@Purdue.edu

#### PROBLEM STATEMENT

To develop a meaningful method of combining risk assessments for individual security Mechanisms in a risk assessment for the overall Layered Solution.

#### RESULTS AND CONCLUSIONS

Function and Class-based Approach to Combining Risk Assessments:

- Promotes modularity and “ease of use”.
- Allows for scalability of risk assessment in Layered Solutions.
- Applicable to Layered Solutions in any Information System

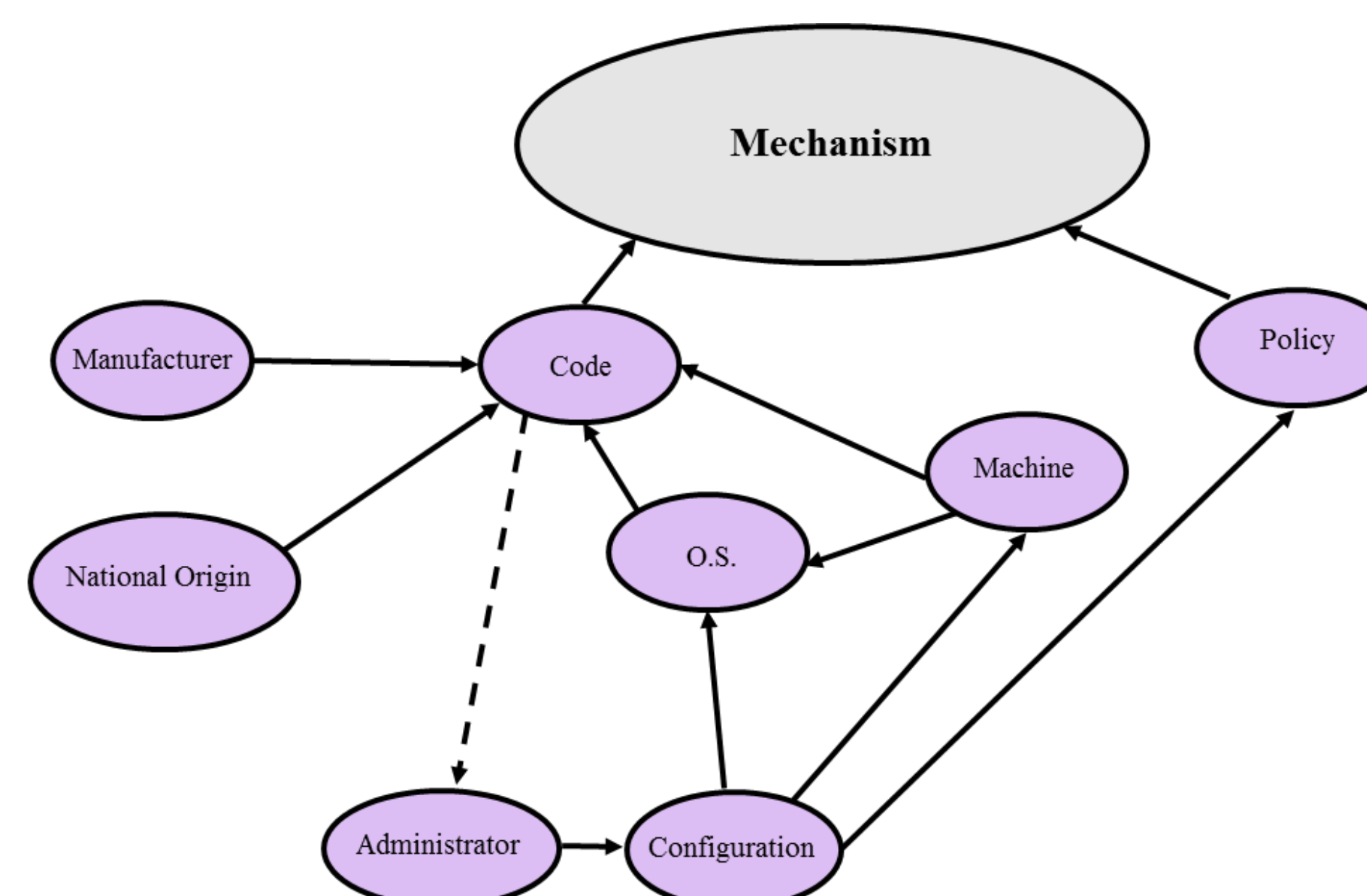
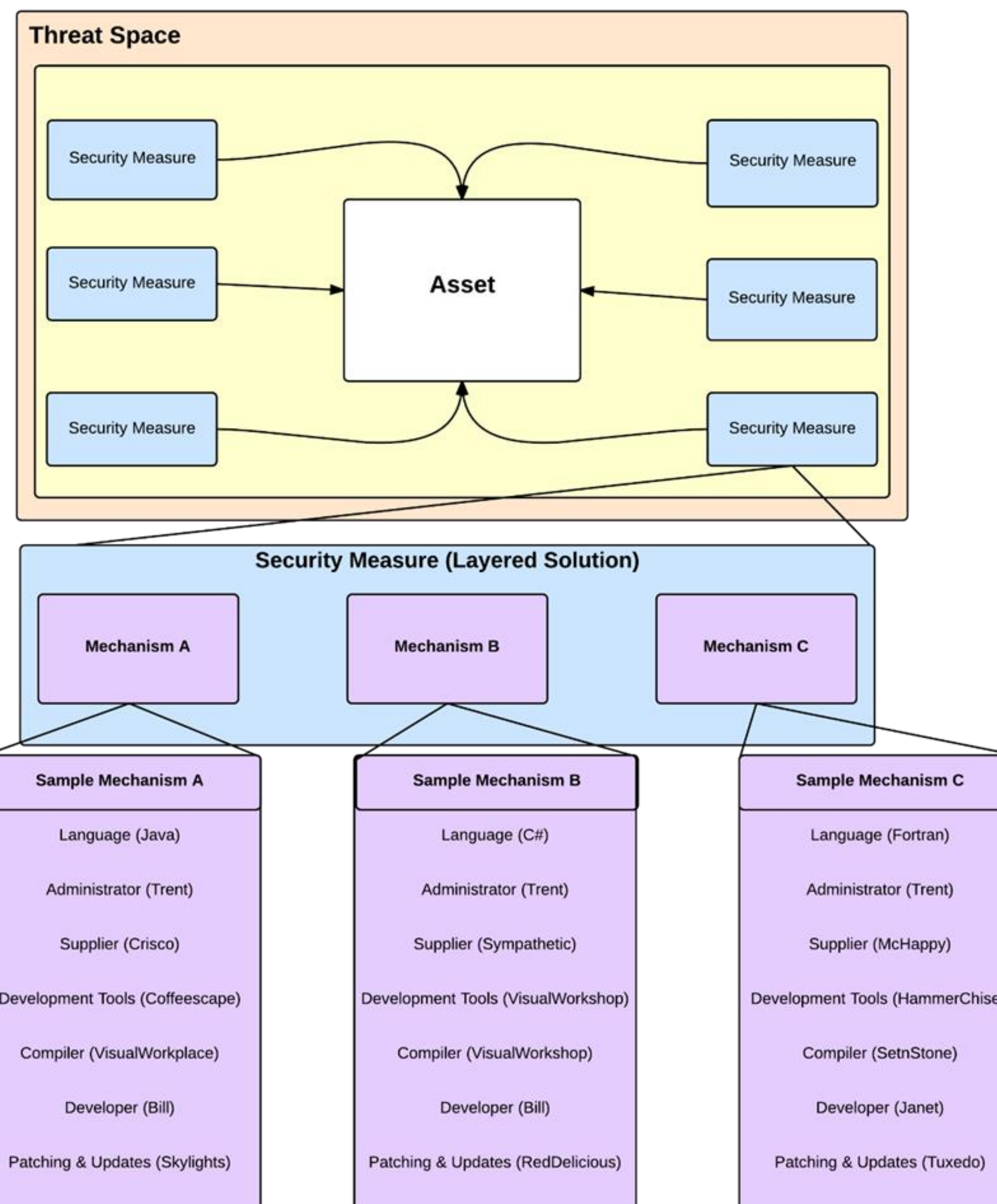
#### FUTURE DIRECTIONS

##### Birthday Paradox

This phenomenon could also exist in cascading vulnerabilities amongst the Mechanisms presented in our model.

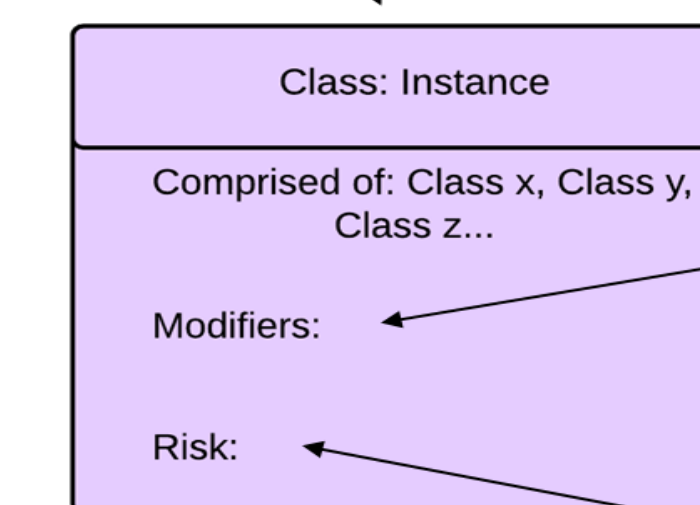
##### Evaluation of Risk

It is possible to represent the risk analysis assumptions as more than simple percentages. In theory, Bayesian scores can be utilized for the assessment of risk at The Security Critical Attribute Object proportion of our model.



#### The Layered Solution Object

The **class** identifies what sort of Mechanism the Layered Solution is using. **Instance** is the specific example of the class.



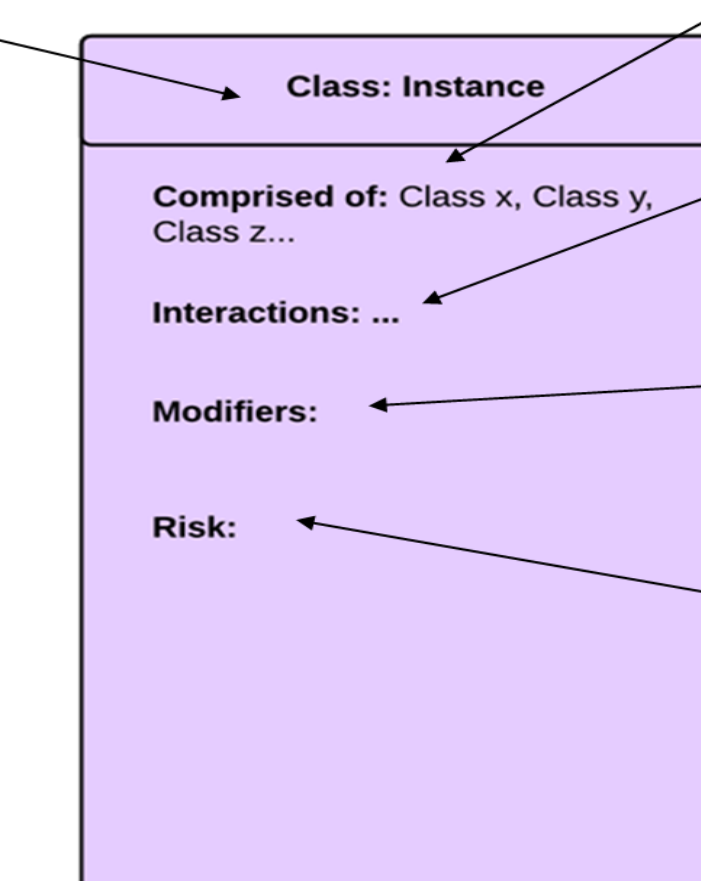
**Comprised of** contains a list of all the Mechanisms that make up the Layered Solution.

**Modifiers** contains any special rules that may need to be applied to this specific implementation

**Risk** is what contains the risk score generated by the model.

#### The Mechanism Object

The **class** identifies what sort of Mechanism the Layered Solution is using. **Instance** is the specific example of the class.



**Comprised of** contains a list of the Security Critical Attributes of the Mechanism.

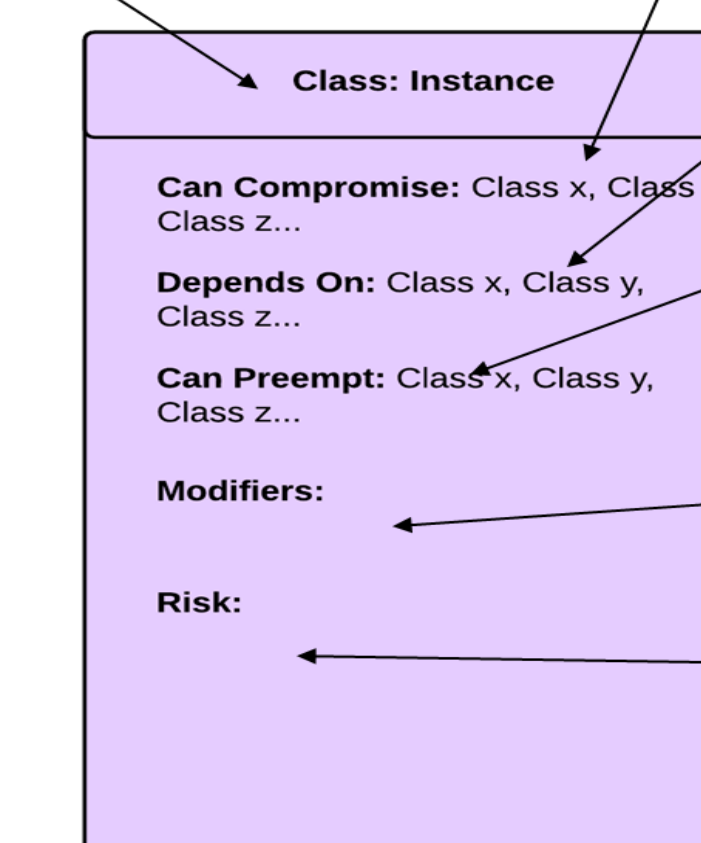
**Interactions** defines the type of interactions the Mechanism can have with other Mechanisms.

**Modifiers** contains any special rules that may need to be applied to this specific implementation.

**Risk** is what contains the risk score of the Mechanism.

#### The Security Critical Attribute (SCA) Object

The **class** identifies the Security Critical Attribute in the Mechanism. **Instance** is the specific example of the Security Critical Attribute.



**Can Compromise** is the first field representing interaction between different SCA's.

**Depends on** is an alternative way of defining the interaction from the other direction.

**Can Preempt** functions same as the compromise field. It contains a list of SCA's that can be preempted by this layer.

**Modifiers** lists the modifications or specific changes.

**Risk** - risk assessments by Subject-matter Expert (SME) in order to define this value