**Ontology Based Approach for Perception of Network Security State (2010)**

Attack

Attack Goal

• Change Data Attack Goal

• Destroy Data Attack Goal

• Disrupt Data Attack Goal

• Steal Data Attack Goal

• Springboard for other attack Goal

Automation Level

• Manual

• Automatic

• Semi-Automatic

Effects

• Null

• Minor Damage

• Major Damage

• Catastrophic

Proposed Ontology

Class **network** has “**provides**” relationship with class **service**.

Class **Attack** has “**has**” relationship with “**Attack goal**”, “**Attack mechanism**”.

Class **Attack** has “**exploits**” relationship with “**Vulnerability**”.

Class **Attack** has “**effects**” relationship with “**services**”.

Class **Attack** has “**performedby**” relationship with **Attack\_Actor**.

Class **Actor** has “**has**” relationship with Class **Actor\_location**.

Class **Actor** has “**is-a**” relationship with Class **user**.

* Current Network vulnerabilities are **inferred** from the class network whose components NOS, Hardware components are related with “**has**” relationship to vulnerability class.
* Each vulnerability **inferred** gives and attack vector.
* This attack vector is **inferred** by relationship “**usedby**” of class vulnerability and class attack. Inverse relation is Attack “**uses**” vulnerability.
* These relations are used to **infer** attack vector of each vulnerability. Each attack has **actor\_location**, **automation level**, **goal**, **scope** and **effect**.

Prediction rules:

Prediction rules are of the following form:

If (actor\_location is foreign) AND (automation level is automatic) AND (Goal is to destroy data) AND (scope is large network) AND (effected service is more than threshold value) then state is unsafe.

Or

If (actor\_location is local) AND (automation level is manual) AND (Goal is to read data) AND (scope is small private network) AND (effected service is less than threshold value) then state is moderately safe.