

CySeMoL/EAAT bugs reported

CySeMoL and EAAT is no longer developed or maintained. So if you are using it, previously identified bugs might be of interest.

Thanks to Rick Hindriks:

1.CySeMoL: Some attack steps are orphans (have no parent)

-> BypassDetectionSystems

-> NetworkVulnerabilityScanner

-> Manually fixed by observing the role in the CySeMoL class model

2.EOM: Entry point relation name is not serialized

-> Defaults to the first option when there is more than one entry point to the same target

3.EOM: Multiple entry points to the same target are loaded as one

-> In combination with (2), this behaviour remains the same

4.EOM: Evidence of multiple template objects of the same type is not differentiable when serialized

-> Possible to store evidence which is both true and false

-> Last evidence in EOM file is applied to all instances

5.PRM spec: multiple inconsistencies in the P2AMF documentation (Class Modeler & Object Modeler user manual August 2013)

-> Verified using the OCL console in the class modeller

-> Gamma: Scale and Shape parameters are swapped (implementation is correct)

-> Gamma: non-cumulative

-> Exponential: mean is specified, but implementation uses lambda.
