ASTo: A tool for Security Analysis of IoT systems

By Orestis Mavropoulos,
Haralambos Mouratidis,
Andrew Fish,
Emmanouil Panaousis

University of Brighton, UK

7/6/2017

Structure of the presentation

- Background information about IoT
- Introduction to the tool's modeling language
- Features of the tool
- Future work

What is Internet of Things? 🤔

- Internet of Things (IoT)
- Web of Things (WoT)
- Internet of Everything (IoE)
- Cloud of Things (CoT)
- Internet of Insecure Things (IoI)

IoT definition

- A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. - Rec. ITU-TY.2060

How do we secure IoT? 🤔

- We need a way to reason about IoT.
    - We need a way to model IoT.
        - We need a way to model security aspects of IoT.

Apparatus Framework

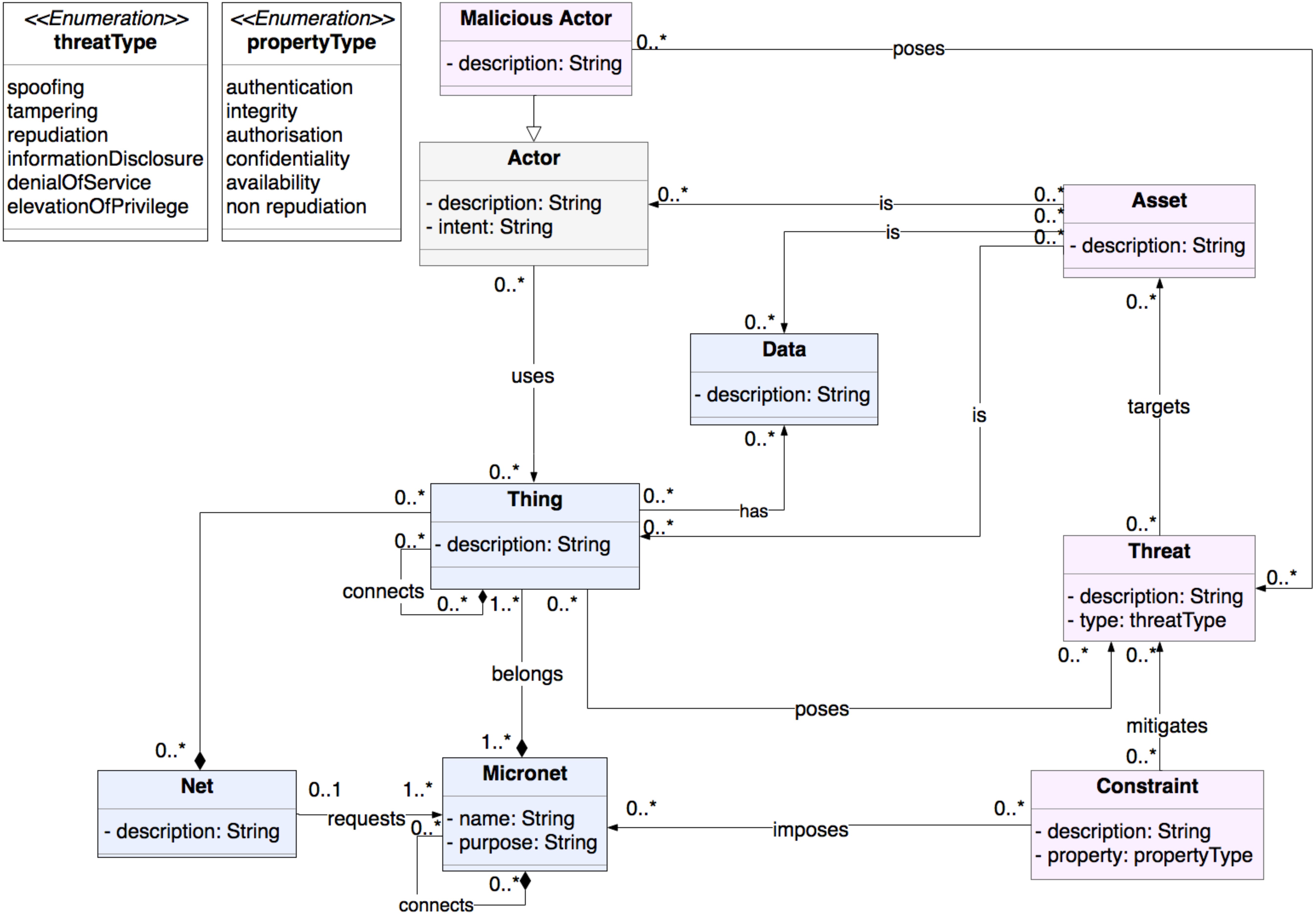
- **Modeling language** to express IoT systems during the design and implementation phases.
- **Modeling procedure** to create IoT models with semantic meaning.
- **Analysis procedure** to identify security issues and propose mitigations.

Characteristics of the Modeling Language

- Concepts are defined using UML classes.
- Concepts are grouped in modules with similar thematic meaning.
- Security analysis is asset-centric.
- IoT systems are considered to be deployed in hostile environments.

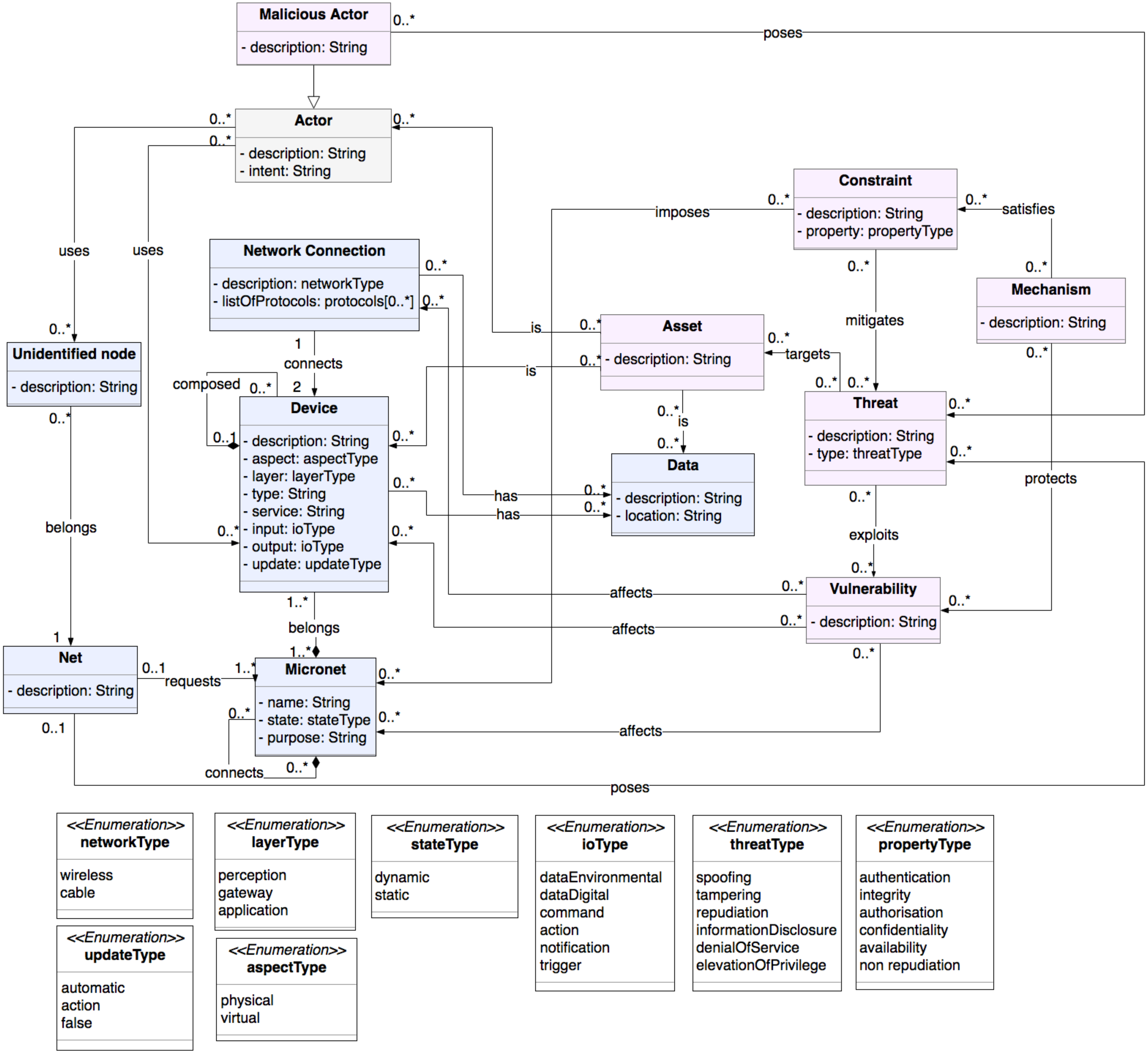
Design Phase Modeling Language

- Used to model an IoT system to "be".
- High-level concepts.
- Used to identify Assets and Threats on a system.
- Can be used to generate high-level security policies.


<<Enumeration>>
threatType
spoofing
tampering
repudiation
informationDisclosure
denialOfService
elevationOfPrivilege
<<Enumeration>>
propertyType
authentication
integrity
authorisation
confidentiality
availability
non repudiation
Malicious Actor
- description: String
0..*
poses
Actor
- description: String
- intent: String
0..*
is
0..*
0..*
is
0..*
Asset
- description: String
0..*
uses
0..*
Data
- description: String
0..*
is
targets
0..*
0..*
Thing
- description: String
0..*
has
0..*
0..*
0..*
Threat
- description: String
- type: threatType
0..*
connects
0..*
1..*
0..*
belongs
poses
0..*
0..*
mitigates
0..*
1..*
0..*
Net
- description: String
0..1
requests
1..*
0..*
Micronet
- name: String
- purpose: String
0..*
imposes
0..*
Constraint
- description: String
- property: propertyType
0..*
connects

Implementation Phase Modeling Language

- Used to model an IoT system at pre-deployment.
- Low-level concepts (extend the Design Phase concepts)
- Used to identify Vulnerabilities of the system.
- Can be used to generate low-level security policies as well as security mechanisms.

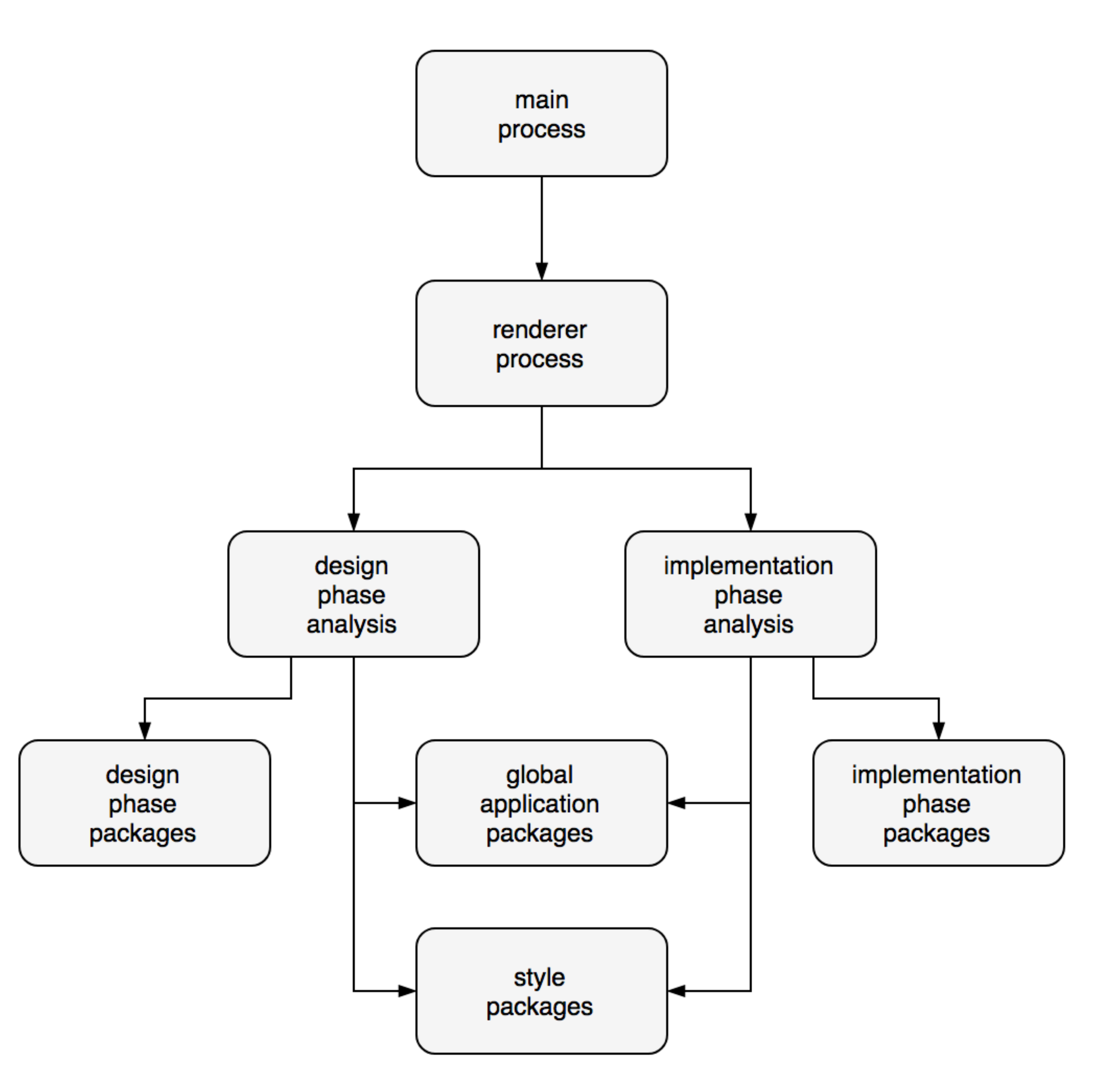

Malicious Actor
- description: String
0..*
poses
Actor
0..*
0..*
0..*
- description: String
- intent: String
uses
uses
Network Connection
- description: networkType
- listOfProtocols: protocols[0..*]
0..*
0..*
1
connects
2
composed
0..*
0..1
Constraint
- description: String
- property: propertyType
imposes
0..*
0..*
satisfies
0..*
Mechanism
- description: String
0..*
mitigates
0..*
Asset
- description: String
is
0..*
is
0..*
0..*
targets
0..*
0..*
Threat
- description: String
- type: threatType
0..*
0..*
0..*
is
0..*
Data
- description: String
- location: String
has
has
0..*
0..*
Unidentified node
- description: String
0..*
0..*
Device
- description: String
- aspect: aspectType
- layer: layerType
- type: String
- service: String
- input: ioType
- output: ioType
- update: updateType
0..*
0..*
0..*
0..*
protects
exploits
0..*
0..*
Vulnerability
- description: String
0..*
0..*
0..*
affects
affects
0..*
belongs
1..*
belongs
1..*
1
Net
- description: String
0..1
requests
1..*
Micronet
- name: String
- state: stateType
- purpose: String
0..*
0..*
0..*
affects
0..1
connects
0..*
poses
<<Enumeration>>
networkType
wireless
cable
<<Enumeration>>
layerType
perception
gateway
application
<<Enumeration>>
stateType
dynamic
static
<<Enumeration>>
ioType
dataEnvironmental
dataDigital
command
action
notification
trigger
<<Enumeration>>
threatType
spoofing
tampering
repudiation
informationDisclosure
denialOfService
elevationOfPrivilege
<<Enumeration>>
propertyType
authentication
integrity
authorisation
confidentiality
availability
non repudiation
<<Enumeration>>
updateType
automatic
action
false
<<Enumeration>>
aspectType
physical
virtual

ASTo's background

- ASTo - Apparatus Software Tool
- Open source project under the MIT license.
- Developed using the Electron framework and the cytoscape.js library.
- Initially developed using the sigma.js library.
- Still in alpha stage.

ASTo's Home

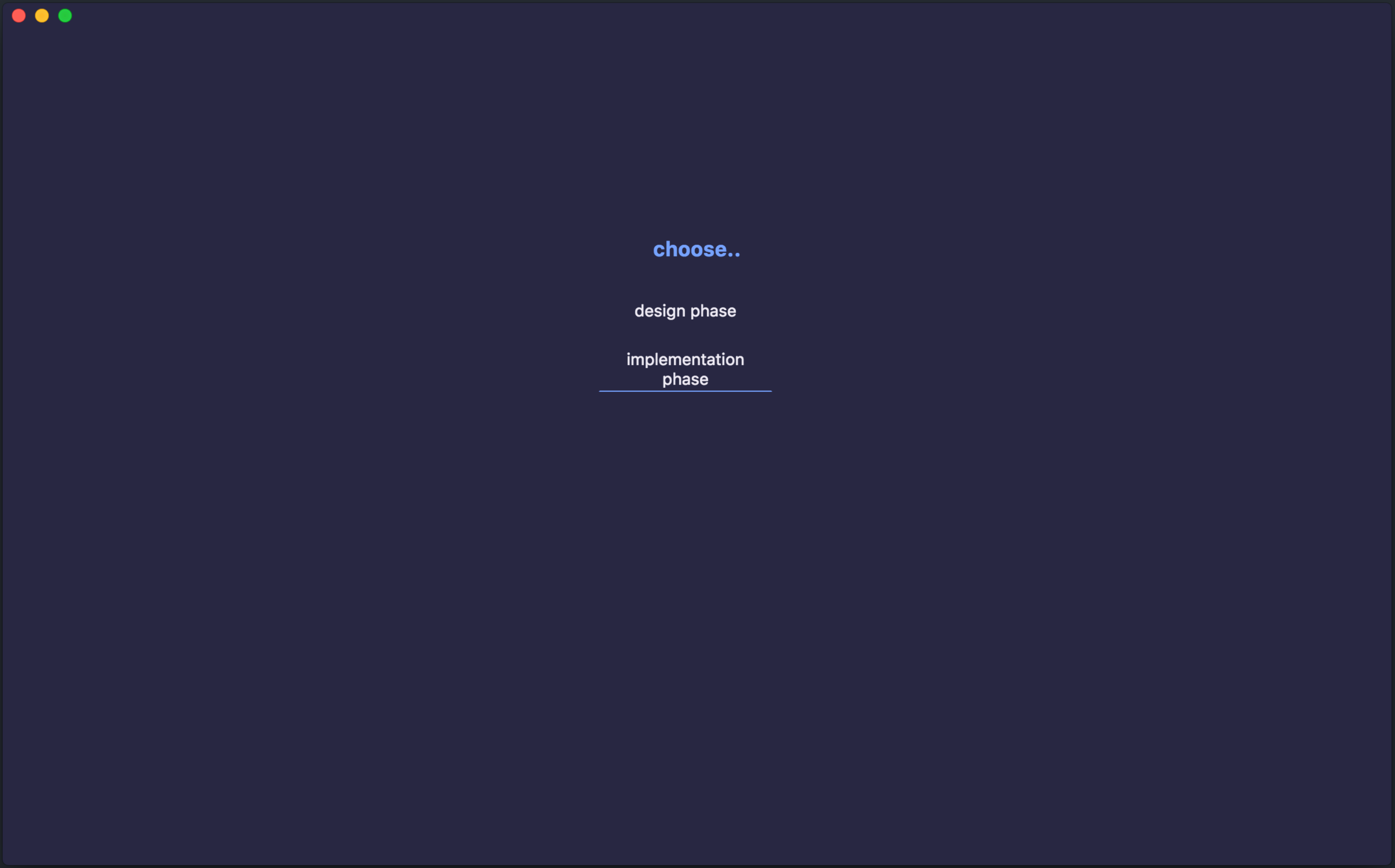
- https://github.com/Or3stis/apparatus
- To built the tool the only requirement is node.js
- Modular and configurable.
- Developed on macOS.
- Works on Windows and Linux, but the GUI will look different.

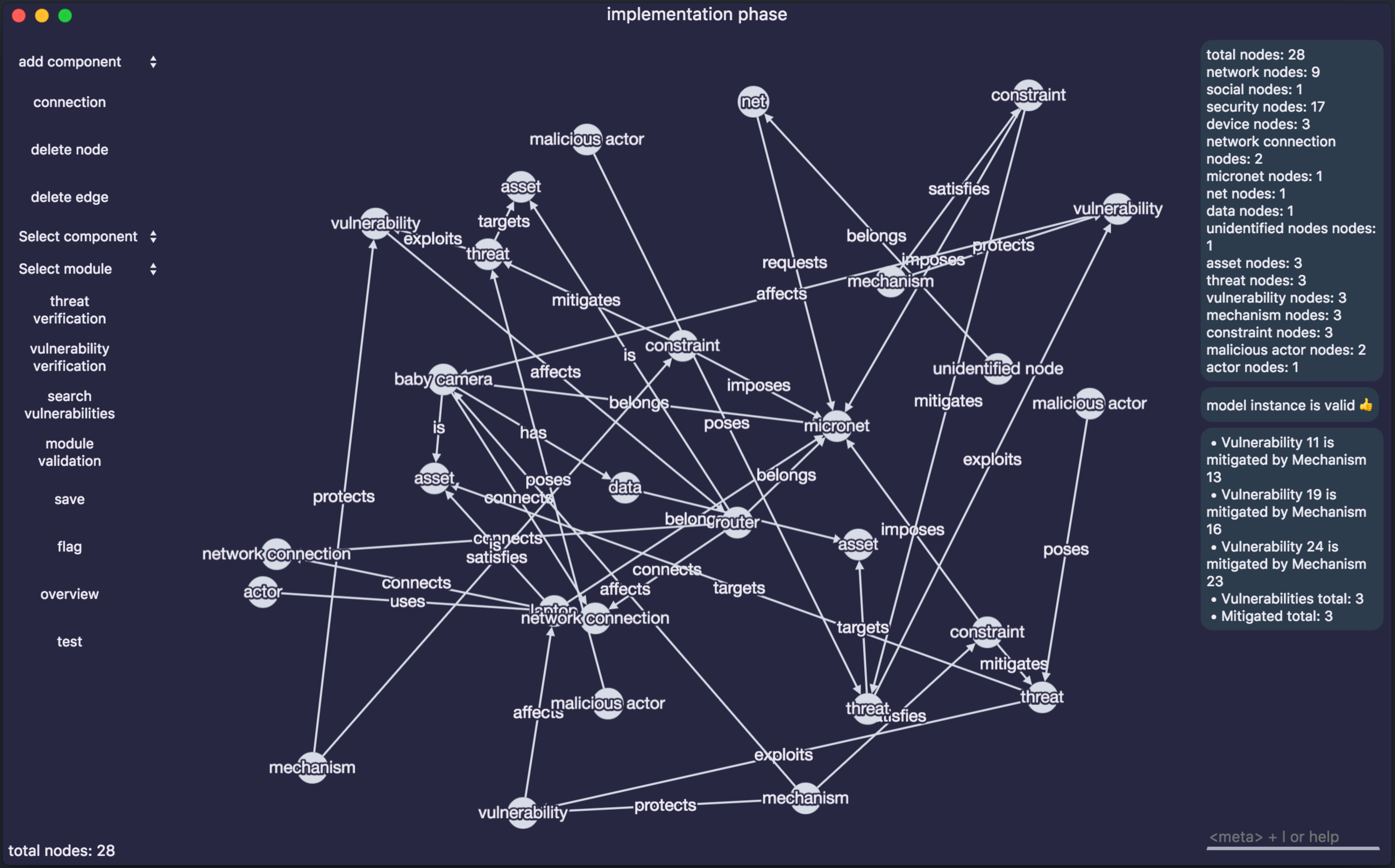

main process
renderer process
design phase analysis
implementation phase analysis
design phase packages
global application packages
implementation phase packages
style packages

ASTo's architecture

ASTo's functionality

- Renders graphs based on the Apparatus metamodels.
- Presents overview of the models.
- Can visualize specific aspects of the models.
- Verifies the integrity of the models.
- Verifies the mitigation impact of the security analysis.
- Identifies patterns in the models.
- and a few more...😉


choose..
design phase
implementation phase



total nodes: 28
network nodes: 9
social nodes: 1
security nodes: 17
device nodes: 3
network connection nodes: 2
micronet nodes: 1
net nodes: 1
data nodes: 1
unidentified nodes nodes: 1
asset nodes: 3
threat nodes: 3
vulnerability nodes: 3
mechanism nodes: 3
constraint nodes: 3
malicious actor nodes: 2
actor nodes: 1

model instance is valid 👍

- Vulnerability 11 is mitigated by Mechanism 13
- Vulnerability 19 is mitigated by Mechanism 16
- Vulnerability 24 is mitigated by Mechanism 23
- Vulnerabilities total: 3
- Mitigated total: 3

total nodes: 28

Future work

- Design & Implementation Phase state machine metamodels.
- Security assistant built in ASTo.

Thank you for listening 😃