GIGL

Group 3 Project - **Tutorial**

Pratam (G)avaravarapu - Rayan (I)ssa - Harshya (G)avaravarapu - Chris (L)imson

GMU CYSE 650 Cyber Risk Modeling and Analysis Tools

Summer 2024 - Alexandre de Barros Barreto, PhD

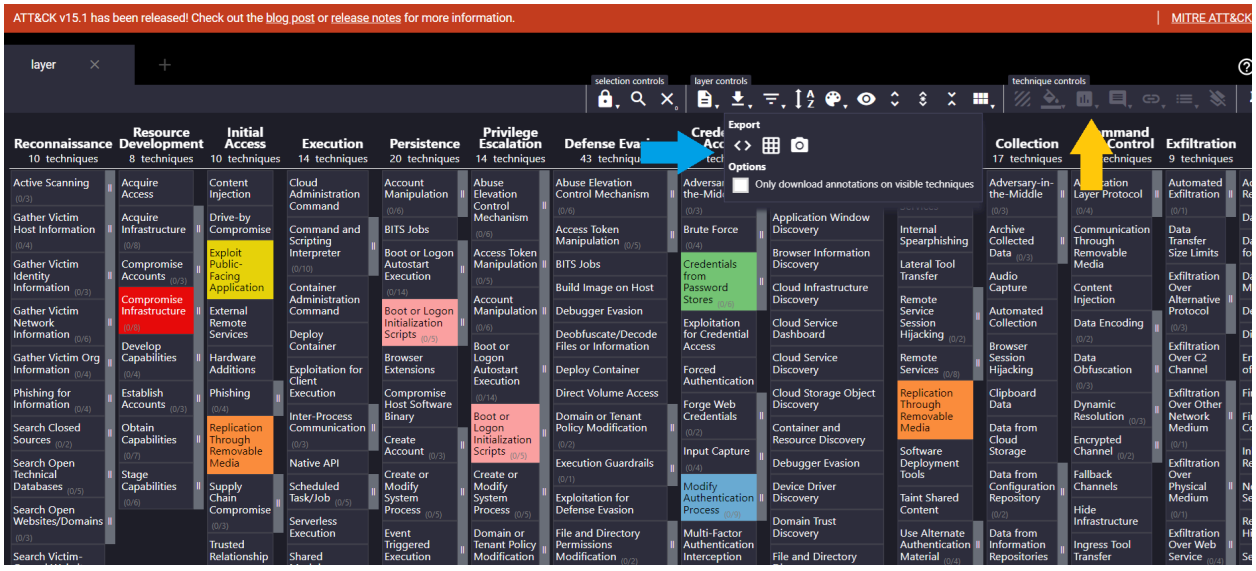
Software that transforms an execution graph path from MITRE ATT&CK into Bayesian representation using the UnBBayes API, incorporating the capacity to elicit and measure uncertainty in the new model representation

1. Setup Endpoint

Browse to UnBBayes modeling framework *https://sourceforge.net/projects/unbbayes* and install. The operation of the tool is outside the scope of this tutorial

2. Prepare Input

Browse to MITRE ATT&CK Navigator, *https://mitre-attack.github.io/attack-navigator* and generate input to GIGL by creating a Layer, highlighting Techniques, assigning each a Score (yellow arrow) and Exporting to JSON (blue arrow). The remaining operation of the web app is outside the scope of this tutorial



3. Download Repository

```
git clone https://github.com/chrimson/GIGL.git
cd GIGL
```

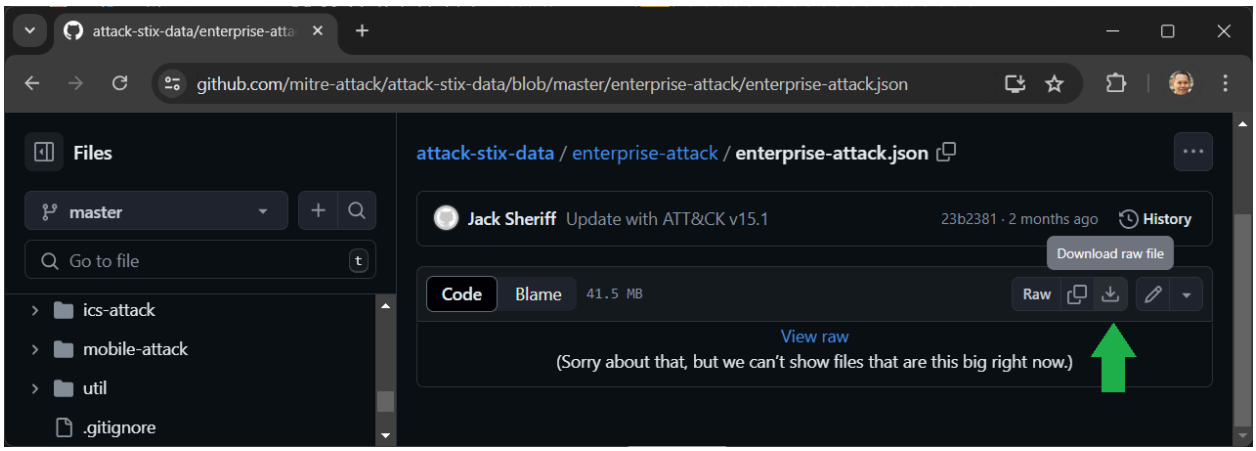
4. Enable Required Dependency

```
pip install pgmpy
```

5. Configure (Optional)

Download latest STIX file (green arrow) at

https://github.com/mitre-attack/attack-stix-data/blob/master/enterprise-attack/enterprise-attack.json



6. Execute

```
python gigl.py mitre.json bayes.net
Mapping techniques from STIX
Bayesian Network model is valid
Bayesian Network exported
```

7. Examine Result

Run UnBBayes and load the output Bayesian Network file