AT-AT – User Manual

Group 8

Anandarajah Yathuvaran

Anil Menon

Dylan Leveille

Eric Leung

Supervisor: Dr. Jason Jaskolka

SYSC 4907 Engineering Project

Department of Systems and Computer Engineering
Faculty of Engineering and Design Carleton
University

Last Updated: February 25, 2022

Table Of Contents

Tree Syntax

This application consumes attack trees in a unique language developed for the tool. This language uses tabs to describe the different levels in a tree and requires that each node in the tree have a name. Parent nodes must have a logical operator (AND or OR) and leaf nodes can be provided metrics that will be used when the tree is analyzed for path severities. Metrics available on leaf nodes are likelihood, victim impact, resource points, and time.

Below are examples of how parent nodes are specified in the language:

1) Open Safe; OR
2) Pick Lock: AND

Both these examples follow the format of <name of node>; OR|AND. The first example made use of disjunction which means at least 1 of its children needs to be executed to open the safe. Whereas with the second example, we make use of conjunction which means we need all its children to be executed to pick the lock.

Below are examples of how leaf nodes are specified in the language:

1) Pick With Bobby Pin
2) Pick With Bobby Pin; l=0.9
3) Pick With Bobby Pin; l=0.9; v=0.3; r=0.8; t=0.1

All three of these examples follow the format of <name of node>; l=#.# | v=#.# | r=#.# | t=#.# | none. As seen in the first example, only a name is required for a leaf node. To improve the analysis of attacks, metrics can be provided as in examples 2 and 3. As many as 4 metrics can be provided; likelihood (l), victim impact (v), resource points (r), time (t). The metric values are in a decimal form between 0.0 - 1.0.

Combining both parent and child nodes can allow a tree to be specified. The following text is an example of what a combination of parent and child nodes could look like:

Open Safe; OR

    Pick Lock; OR

        Pick With Bobby Pin; l=0.9; r=0.2

        Break Lock; l=0.5; v=0.3; r=0.7; t=0.5

    Dynamite; AND

        Add Chemical; r=0.5; v=0.4

        Add Heat; t=0.9; l=0.5; v=0.7

Each tab indicates a new level in the tree and allows for nesting. As seen in the examples, “Pick Lock” and “Dynamite” are both parent nodes, which are themselves children of the “Open Safe” node. In the case of the parent “Pick Lock,” it uses disjunction which means that either an

attacker can “Pick with Bobby Pin” or “Break Lock” for the “Pick Lock” scenario to be achieved. Whereas the parent “Dynamite” uses conjunction which means that the attacker must “Add Chemical” and “Add Heat” for the “Dynamite” scenario to be achieved. However, for the root goal of the attacker to be achieved, either the attacker can “Pick Lock” or “Dynamite” for the tree’s root goal to be satisfied.

Importing a Tree

This tool allows a user to import any preconfigured DSL text file which will automatically fill up the DSL text box. After which, the user is easily able to generate the tree. Here are the steps to import the tree:

Step 1: Click “File”

Step 2: Click “Import DSL”

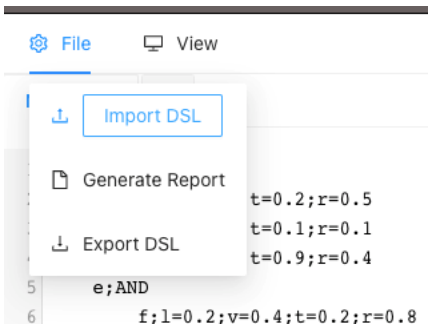

Figure 1: Import DSL

Step 3: Select DSL text file of your choice

Step 4: Click “Generate’

Now you should be able to see the tree generated.

Export Tree

This tool allows a user to export a DSL tree to a text file. After which, the user can import the file. Here are the steps to export the tree:

Step 1: Click “File”

Step 2: Click “Export DSL”

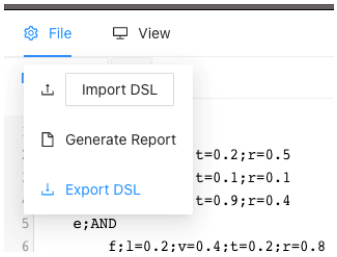

Figure 2: Export DSL

Step 3: Select a file name of your choice

Step 4: Select a location of your choice

Ste 5: Click “Save”

Now you should be able to see the file generated.

Generate Tree

This tool allows a user to manually input an attack tree for generation. Here are the steps to generate a tree:

Step 1: Enter text following the DSL format in the text area such as

```
a;OR
    b;l=0.7;v=0.1;r=0.5;t=0.2
    e;AND
        f;l=0.2;v=0.4;r=0.8;t=0.2
```

Step 2: Click “Generate”

Now you should be able to see the tree generated.

View Attack Scenarios

When an input attack tree is generated, the AT-AT tool also analyzes the tree to generate a list of all possible attack scenarios on the tree. This list can be accessed by clicking on the “Show Scenarios” button shown below:

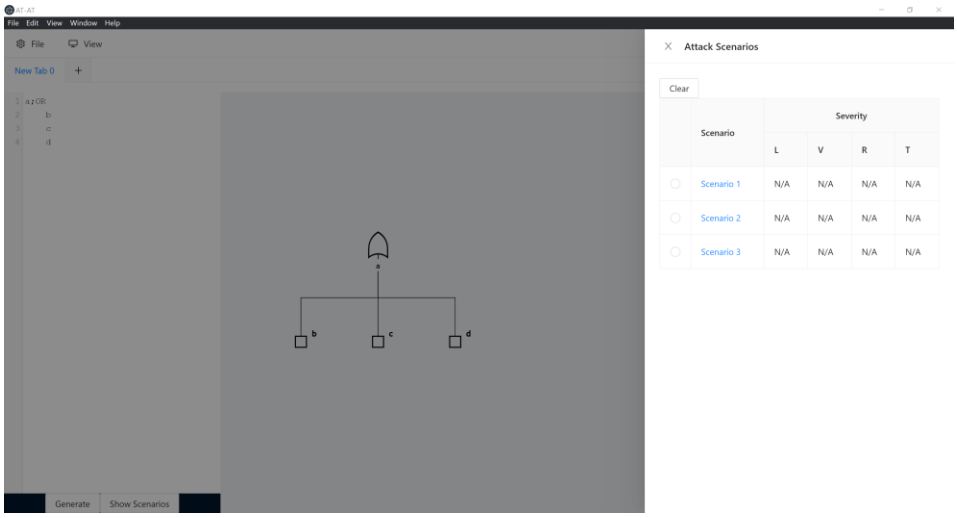

Figure 3: Display Scenarios

A specific scenario from the list of attack scenarios can be selected by clicking the radio button for the associated scenario:

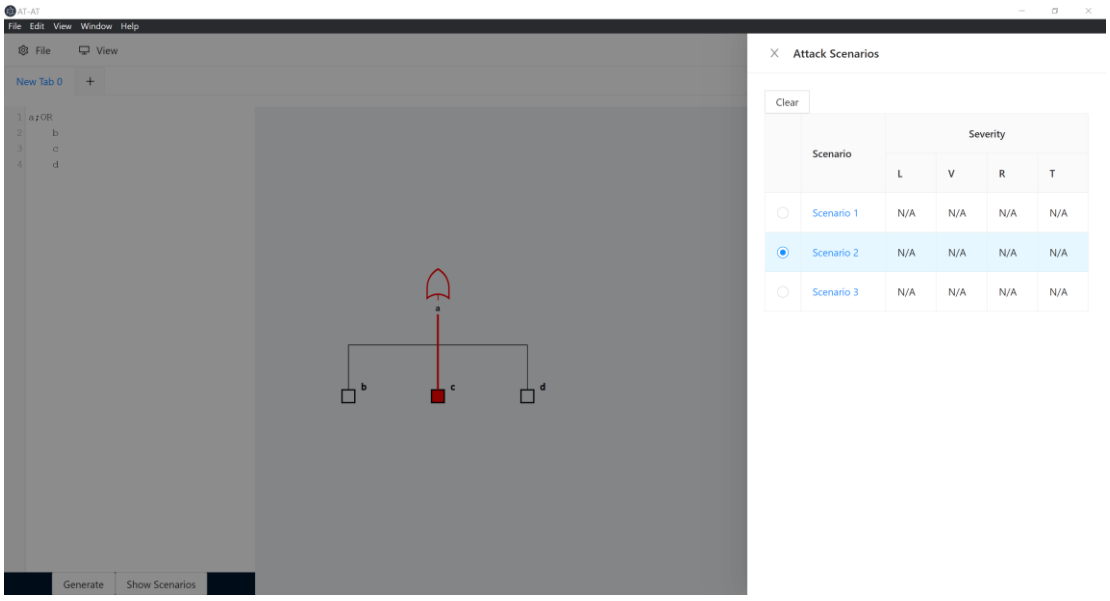

Figure 4: Select Scenario

The attack scenarios list can then be closed by either clicking outside the “drawer” component, or by clicking the “x” button to close the list. This will reveal the path of the selected scenario highlighted in red:

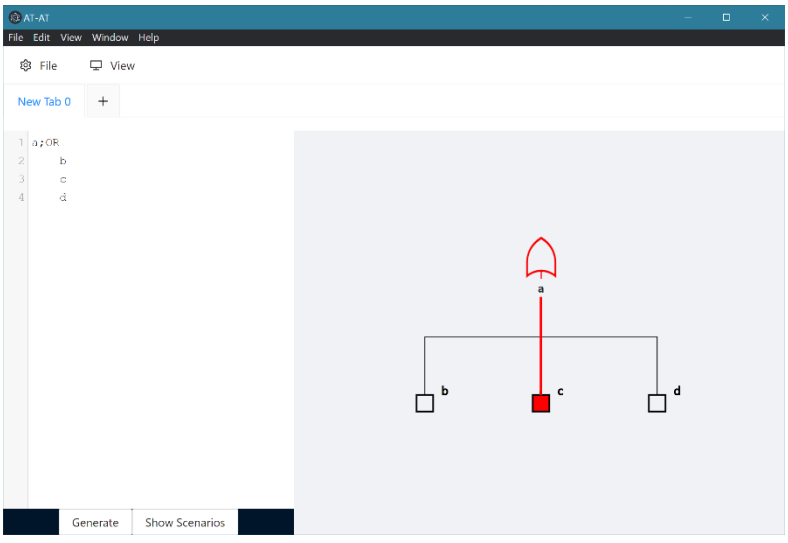

Figure 5: Scenario Highlighting

The attack scenarios list can be displayed again by clicking the “Show Scenarios” list. The “Clear” button can be clicked to remove the selected scenario and return to the default view. Another scenario can be selected to be highlighted as well.

View Recommendations

To view recommendations for an attack scenario, make sure the scenario is first selected. Under the View button, click “Enable Recommendations”.

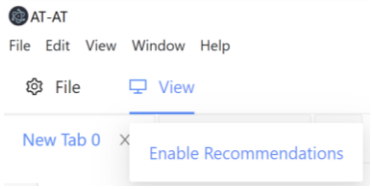

Figure 6: Enable Recommendations

This will make a box appear in which the recommendations for the selected scenario is shown. An example of this is shown below:

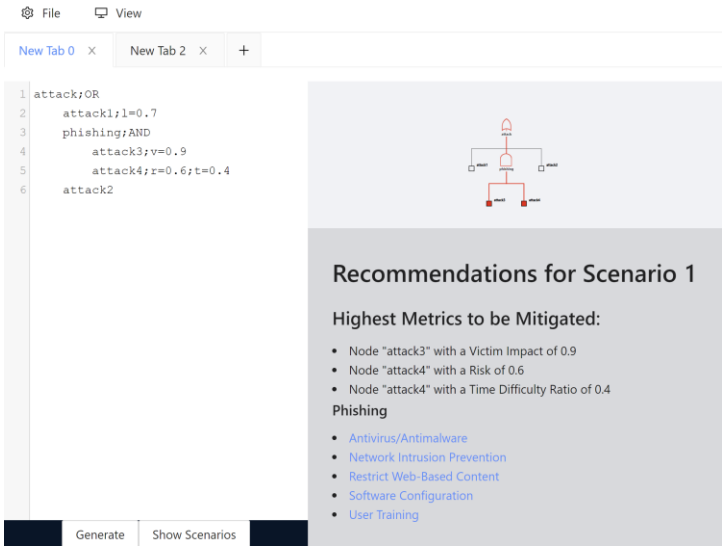

Figure 7: Example Recommendations

This box will inform you of the highest values of each metric found in the attack scenario. It will also inform you of specific mitigations for common attacks that were found in the scenario; it does this by analyzing the text in the nodes of the attack scenario to see if any common attack

keywords are found. In this case, the word phishing was found in the path, hence recommendations to help mitigate phishing attacks are provided.

To remove the recommendations box, similar to how it was enabled, simply click on the View button and “Disable Recommendations”. The box should no longer be visible.

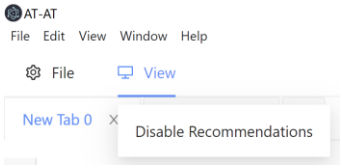

Figure 8: Disable Recommendations

Export Report

This tool allows a user to export their generated tree along with all its scenarios into an html format. That way, a user can save their attack tree and all its analysis into a file that can be accessed whenever it is convenient for them. Here are the steps to exporting a report:

Step 1: Ensure you have either entered some DSL text or imported the DSL text such that a tree is generated.

Step 2: Select “File”

Step 3: Select “Generate Report”

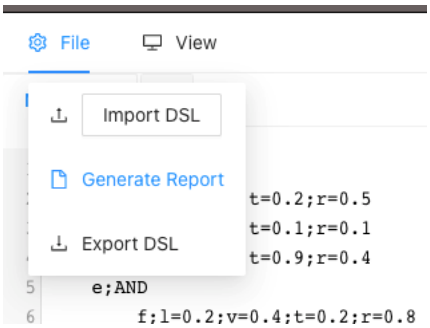

Figure 9: Generate Report Button

Step 4: Select “Save Report”

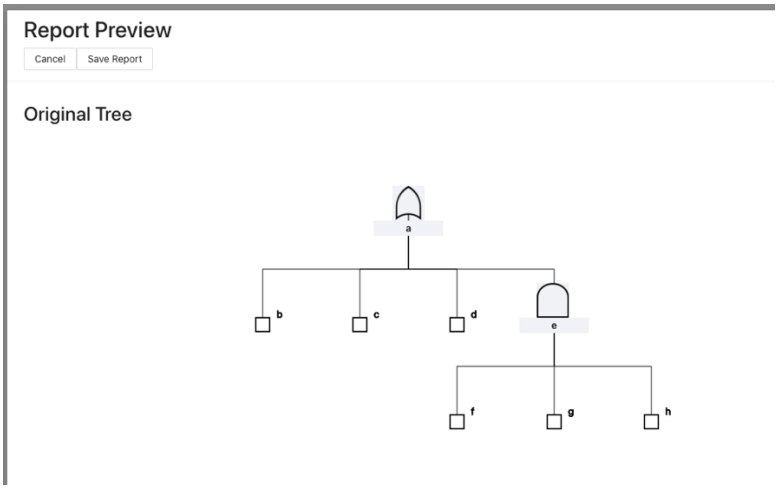

Figure 10: Report Preview

Step 5: Choose destination folder

Step 6: Filename name must end with .html

Step 7: Click “Save”

Now a user is able to open the file on their favorite web-browser and view the generated report.

Multiple Trees

The user is able to generate multiple trees on the same application by adding multiple tabs. Here are the steps for having multiple trees:

Step 1: Insert DSL text on current tab (New Tab 0)

Step 2: Click “Generate”

Step 3: Click “+” on the top left corner to add another tab

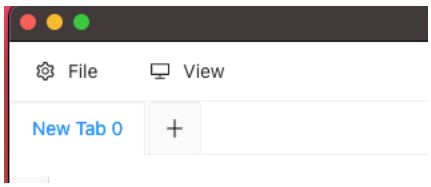

Figure 11: Select New Tab

Step 4: Repeat steps 1-3 depending on the number of trees the user wants to generate simultaneously.

The user is able to view multiple trees by switching tabs to conduct their analysis.