TREE Visualizer Design and Development

Revision History:

Revision Number	Description	Author	Timestamp
V0.1	Initial Draft	Loc Nguyen	06/14/2013

Contents

1 Overview of TREE Visualizer

The visualizer component of TREE is the interface to allow for representation of the trace and taint information in graph format. Through the graph format, the taint relationships will be depicted through edge relationships with each graph node representing a single taint.

2 Data Design

The taint data is stored within a taint object data structure within memory that couples the taint attributes and edge relationships between taint objects. Further taint objects store edge relation attributes for children nodes, where the attributes pertains to the taint policy.

Currently the taint information is passed through to the visualizer in the form of a uniquely named text file. The text file is line-delimited and generated by the Analyzer component with the taint policy as the primary differentiating factor amongst taint graphs.

3 Architecture

The taint data is stored within a taint object data structure within memory that couples the taint attributes and edge relationships between taint objects. Further taint objects store edge relation attributes for children nodes, where the attributes pertains to the taint policy.

There are currently two concurrent graphing systems available in the visualizer, the IDA Pro grapher(WinGrapher) and a QT-based grapher. For the QT-based grapher, the layout algorithms currently rely on Scipy/Numpy in order to determine node and edge placement on a QT GraphScene.

4 Interface

Taint nodes, as seen through the IDA Graph are currently uniquely distinguished by their name and color designation for nodes.

- Green - Input taint nodes
- Pink - Register taint nodes
- White - Memory taint nodes
- Red - Sink nodes

The visualizer's other focus point is the taint table. Children nodes are clickable and will show the sequence of taints through contextual highlighting of taint nodes within the table. The highlighting will allow a user to follow the flow of taints within a particular chain.