Taint-enabled Reverse Engineering Environment (TREE)

Taint-enabled Reverse Engineering Environment (TREE)

What is TREE?

Description of TREE

- Lixin Li [lil@battelle]
- Xing Li [lix@battelle.org]
- Loc Nguyen [nguyenl@battelle.org]

On this page

Components

- /Tree_Analyzer.py - Main component for the analyze/visualizer widgets
- /Tree_Tracer.py - Main component for the tracer widget
- /dispatcher/* - Core compoent for TREE
- /documentation/*

Getting Started

Requirements

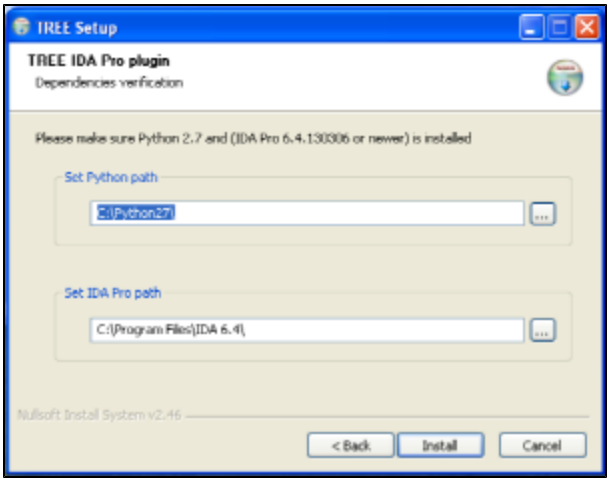
Windows XP SP3 - Tested and Verified
Windows 7 64bit - Tested and Verified

Requirements

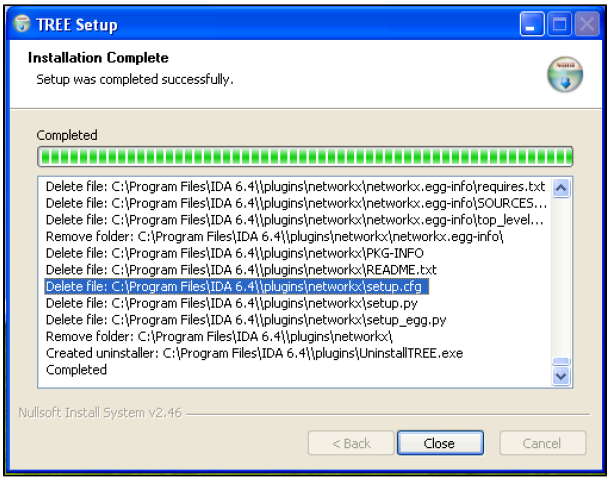
IDA Pro 6.4.130306 or newer
Python 2.7
NetworkX - *Installed by the TREE installer*
PySide for IDA Pro - *Installed by the TREE installer*

Installation

>Locate and run InstallTREE.exe



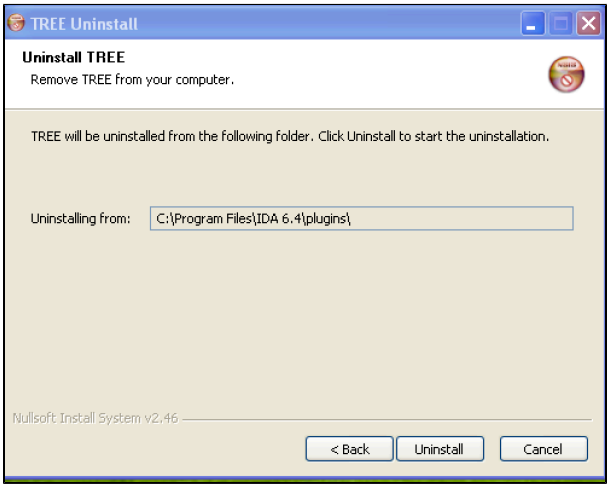
>Verified the IDA Pro and Python installed path or browse to the correct path



>Close the installer. The TREE plugin should be installed at this point.

Removal

>Locate and run uninstallTREE.exe *(This file is usually located in your IDA Pro plugins folder)*

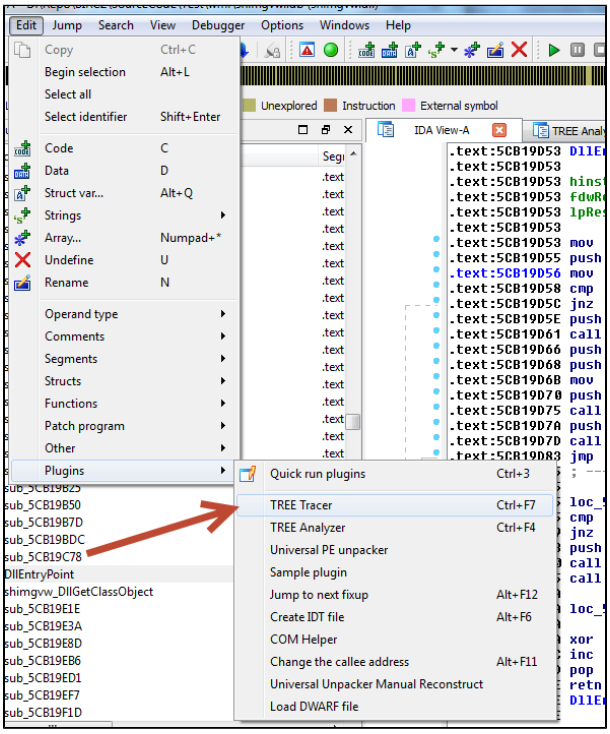


Usage

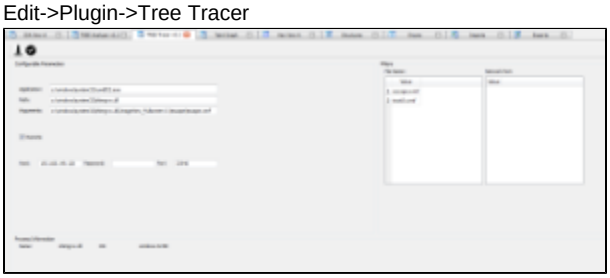
Initializing TREE

Tracer

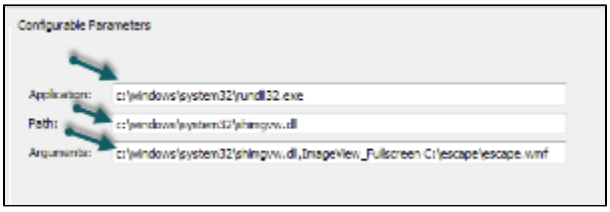
- Launch IDA Pro to disassemble a new file
  - (Previously, we reused old .IDB files but we cannot now because we take a snapshot of the process' memory each time we generate a Trace)
- ***On Windows 7***
  - Should run IDA Pro with Admin privileges, this will allow the Tracer to save configuration parameters



Edit->Plugin->Tree Tracer

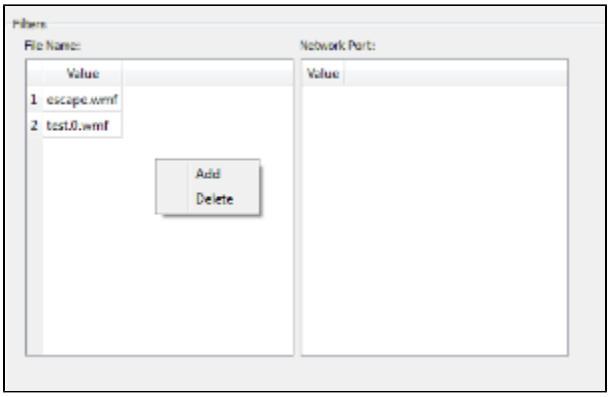


Typically the application location and the path will be the same for the target, but there can be cases where they may differ such as running a DLL. Arguments to the target can also be inputted.



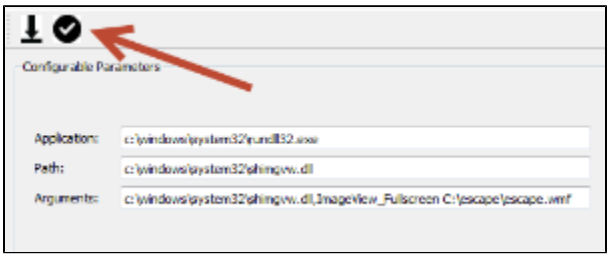
For remote debugging, check the remote checkbox and input the network information to reach the machine.

Filters for file names and network ports can be specified through the right-click menu on each respective table.



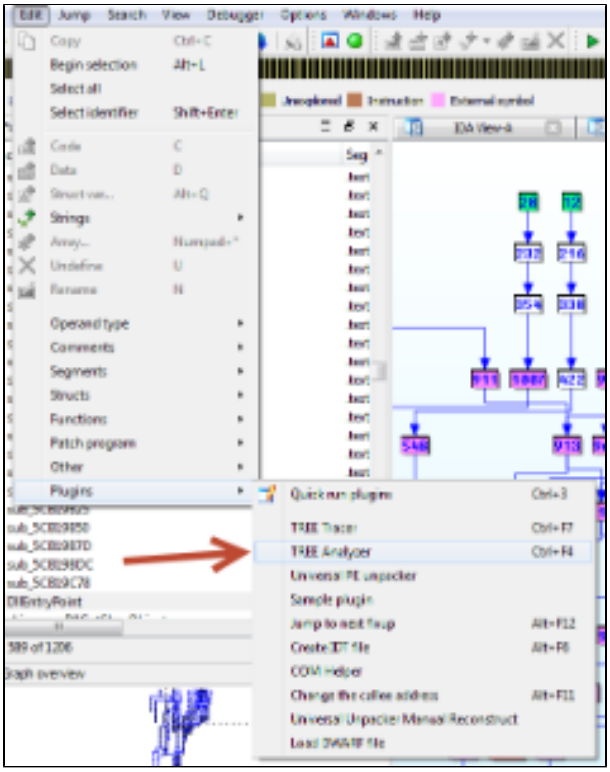
Configuration details have to be manually saved, but will remain persistent between sessions.

Start the trace.



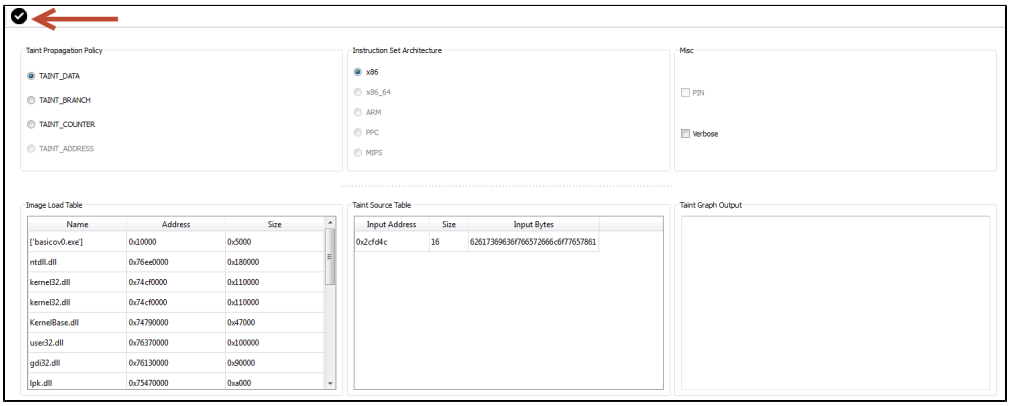
If IDA is selected as the debugger, IDA will isolate the debugging mode from all other plugins - as a consequence the Tree Tracer component will crash and will have to be reinitialized after a trace is complete. Reload the IDB file, the original IDB state will have been saved to a backup file - the IDB will now contain the trace information.

Analyzer



Edit->Plugin->Tree Analyzer

The analyzer has to be manually invoked after the tracing step is finished. The trace information is now stored within the IDB file.

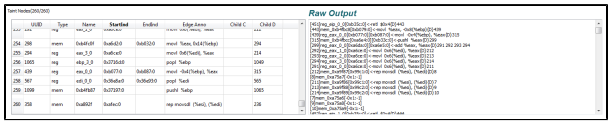


Select a taint propagation policy(default being taint_data):

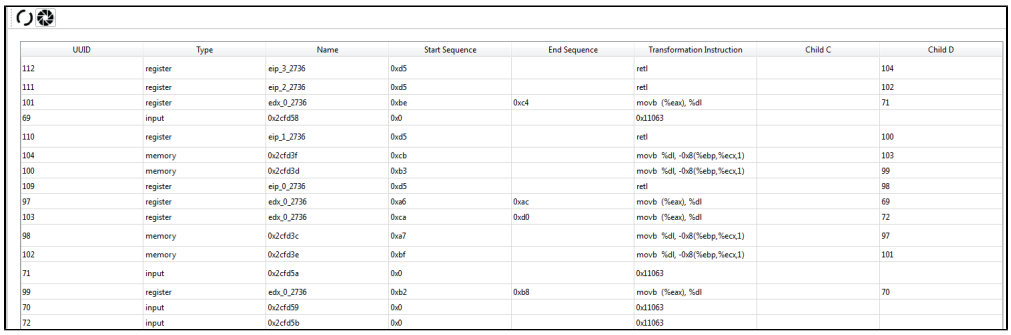
Select an instruction set architecture and optionally select verbose for extended output.

Start the analyzer after inputting the appropriate options

The taint data is rendered into a table alongside a textbox containing the raw output of the results.



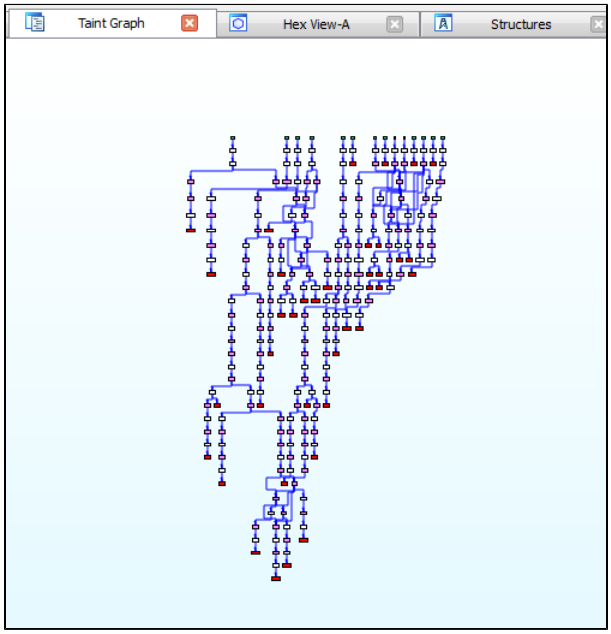
Visualizer



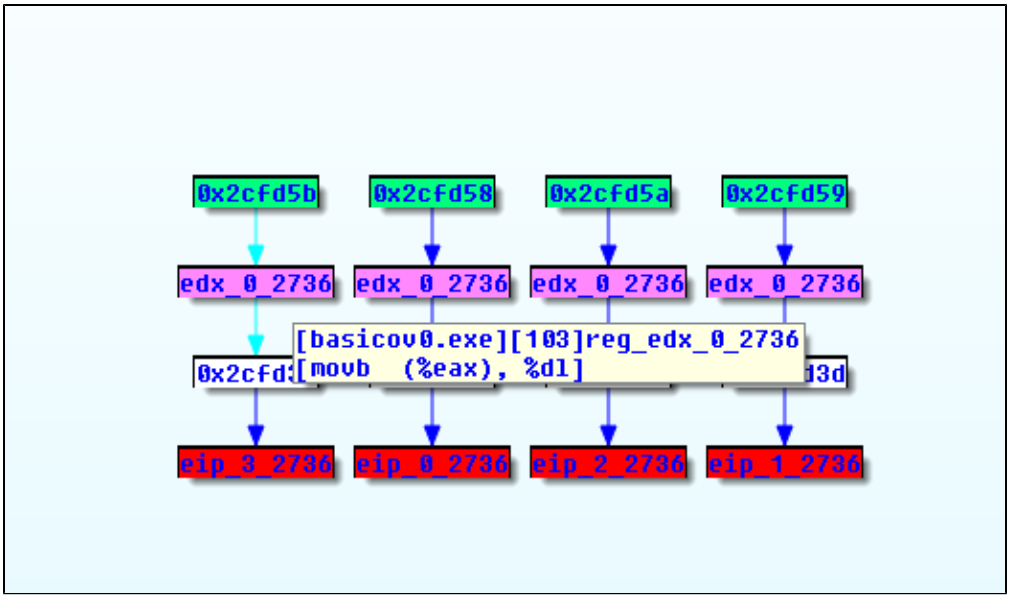
UUID	Type	Name	Start Sequence	End Sequence	Transformation Instruction	Child C	Child D
112	register	eip_3_2736	0xd5		retl		104
111	register	eip_2_2736	0xd5		retl		102
101	register	edx_0_2736	0xbe	0xc4	movb (%eax), %dl		71
69	input	0x2cfd58	0x0		0x11063		
110	register	eip_1_2736	0xd5		retl		100
104	memory	0x2cfd3f	0xcb		movb %dl, -0x8(%ebp,%ecx,1)		103
100	memory	0x2cfd3d	0xb3		movb %dl, -0x8(%ebp,%ecx,1)		99
109	register	eip_0_2736	0xd5		retl		98
97	register	edx_0_2736	0xa6	0xac	movb (%eax), %dl		69
103	register	edx_0_2736	0xca	0xd0	movb (%eax), %dl		72
98	memory	0x2cfd3c	0xa7		movb %dl, -0x8(%ebp,%ecx,1)		97
102	memory	0x2cfd3e	0xbf		movb %dl, -0x8(%ebp,%ecx,1)		101
71	input	0x2cfd5a	0x0		0x11063		
99	register	edx_0_2736	0xb2	0xb8	movb (%eax), %dl		70
70	input	0x2cfd59	0x0		0x11063		
72	input	0x2cfd5b	0x0		0x11063		

Extended taint table view allows user to manually follow taints and their children. The flow of a taint can be highlight by selecting a child cell, children rows will be highlighted.

Start the IDA grapher



Unfortunately IDA grapher only supports one zoom level which can be reached through the right-click menu.



Related

- *Link to any related Knowledge Base articles or External Links*
- *One way to improve this template is by replacing "Related" with either the related-labels or contentbylabel macro*