# TREE PIN Tracer Support

## Purpose:

Provide a faster tracing alternative than IDA Debugging, which can be very slow.

## Main advantages:

* Fast: PIN is optimized for instrumentation and tracing, so it generally much faster than debugging alternative.
* CBASS execution PIN tracer (exetrace.dll) can track input at system call level so it capture much more comprehensive inputs from file and network than Win32 API level.
* CBASS execution PIN tracer (exetrace.dll) uses binary encoding and instruction map to reduce redundancy in trace file, so the trace file is significantly smaller.

## Main limitations:

* PIN only supports x86 on Windows/Linux, and CBASS execution PIN tracer only supports Windows (which can be ported to Linux relatively easy)
* CBASS PIN Tracer capture input at Windows system call level that varies with Windows kernel versions; so far it supports Windows XP, 2003, Vista up to Win7 base version but not working with current Windows 7 yet. Tracing not depend on input can work on current versions.
* CBASS PIN Tracer currently supports one file filter and no network filter.

## TREE PIN Tracer Setup:

To simplify setup process, here are a couple of assumptions:

* Pin runtime (under 3rdPartyTools folder in the Repo) will be created in the root of C drive in the target VM (or local host if running target locally). So there should be a c:\pin folder after installation.
* To connect TREE GUI and the *PINed* Target, a utility program called PinAgent is developed and checked in under TREE\dispatcher\core\structures. PinAgent works like IDA remote debug stub. PinAgent needs to start before real target program runs. At PinAgent start time, it will print out the target machine IP address and the port it listens to (23966), then wait for PIN trace request and invoke PIN with right command line and taint filters.
* To avoid sending trace files back and forth between TREE GUI and target machine, a shared folder named TREE-TRACE is mapped to Z:\TREE-TRACE inside target VM. CBASS PinTracer will save trace files into that folder.
* When CBASS PinTrace finishes trace generation, PinAgent will send a Trace Ready message back to TREE GUI, so TREE GUI can notify user to move on to next stage.

## Sanity Tests:

* Sanity tests have been performed for BasicOV, WMF and winVS on Windows XP SP3 and SP2, traces for these cases are confirmed.

## TODO:

* Update installation process to include PIN tracer components.(Xing)
* Update User Manual so user is aware of the right setup. (Loc)
* Update Tracer GUI for new configurations and enhance usability.(Xing)
* Develop new PIN-trace parser and integrate with Taint Analyzer. (Nathan)