Αρχιτεκτονική Υπολογιστών – Εργαστήριο

PIN Tools (Dynamic instrumentation of programs)

Τι σημαίνει Instrumentation

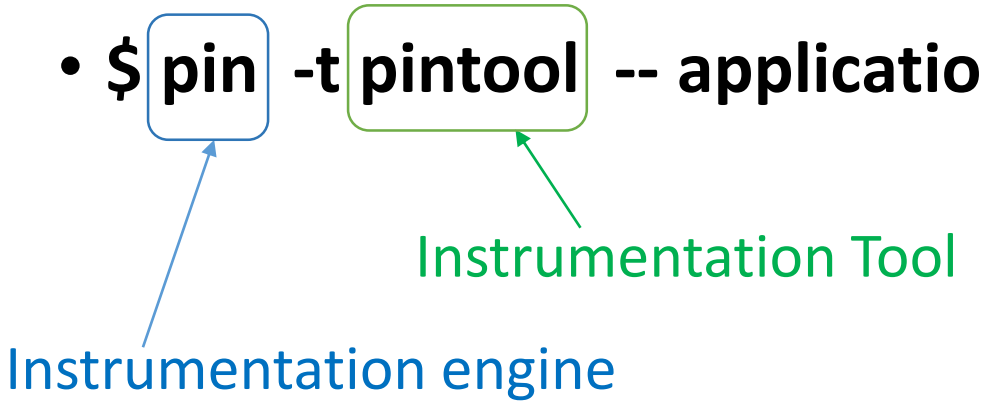
- Είναι μία τεχνική η οποία εισάγει έξτρα κώδικα σε ένα πρόγραμμα ώστε να συλλέξουμε πληροφορίες κατά την εκτέλεσή του
- Τεχνικές Instrumentation
  - Instrumentation σε επίπεδο πηγαίου κώδικα
  - Instrumentation σε επίπεδο κατευθείαν σε εκτελέσιμο κώδικα/πρόγραμμα

Χρησιμότητα του δυναμικού Instrumentation

- Δεν υπάρχει ανάγκη για επανα-μετάφραση ή σύνδεση με βιβλιοθήκες
- Διαχείριση κώδικα κατά τον χρόνο εκτέλεσης
- Προσαρμογή σε διεργασίες που εκτελούνται δυναμικά

Χρήση του Pin

- **$ pin -t pintool -- application**



- **$ pin –t pintool –pid 1234**

Instrumentation vs. Analysis

- **Instrumentation routines** ορίζουν σε ποιο σημείο θα εισαχθεί το instrumentation
  - Για παράδειγμα πριν από μία εντολή
  - Το instrumentation συμβαίνει την **πρώτη φορά** που θα εκτελεστεί μία **εντολή**
- **Analysis routines** ορίζουν τι πρέπει να γίνει όταν ενεργοποιηθεί το instrumentation
  - Για παράδειγμα: αύξηση ενός counter
  - Η ανάλυση συμβαίνει **κάθε φορά** που εκτελείται η εντολή

Pintool: μέτρηση εντολών

```
sub $0xff, %edx
counter++;
cmp %esi, %edx
counter++;
jle <L1>
counter++;
mov $0x1, %edi
counter++;
add $0x10, %eax
counter++;
```

Χρήση και Output

- **$ /bin/ls**

  Makefile imageload.out itrace proccount

  imageload inscount0 atrace itrace.out

- **$ pin -t inscount0 -- /bin/ls**

  Makefile imageload.out itrace proccount

  imageload inscount0 atrace itrace.out

Count 422838

Downloading & Installing Pintool (3.26 Jan'23)

- https://www.intel.com/content/www/us/en/developer/articles/tool/pin-a-binary-instrumentation-tool-downloads.html
- Linux:

  $ tar zxf pin-3.2-81205-gcc-linux.tar.gz
  $ cd pin-3.2-81205-gcc-linux

To build and run a sample tool on Linux*:

cd source/tools/SimpleExamples
make obj-intel64/opcodemix.so
../../../pin -t obj-intel64/opcodemix.so -- /bin/ls

This will instrument and run /bin/ls, the output for this tool is in opcodemix.out