Contents

1 Overview 1

2 Source Code Instrumentation 2

3 Bytecode Instrumentation 3

4 Machine Code Instrumentation 7

5 Instrumentation Overwriting Code 8

6 Instrumentation Translating Code 13

1 Overview

Instrumentation

Purpose
Instrumentation inserts measurement code (probes) into well defined program locations to facilitate data collection.

Examples of instrumentation:
- Static instrumentation in source files
- Static or dynamic instrumentation in bytecode
- Static or dynamic instrumentation in machine code
- Static preparation in source files that allows dynamic instrumentation in machine code

Instrumentation

Collected Information
Information that is interesting but cannot be measured directly:
- Precise program traces
- Program state snapshots
- Function parameter values
- Anything else the program can observe ...

Applications
Useful for many dynamic analyses:
- Test coverage
- Race detection
- Taint tracking
- Origin tracking
- Memory usage checks
2 Source Code Instrumentation

**Source Code Instrumentation**

**Benefits**
- Relatively easy to insert
  - Source code is made to be modified
  - Automated tools sometimes struggle
- Program state naturally available
- Locations relevant to code structure

**Challenges**
- Instrumentation is subject to compiler optimization:
  - Optimized together with surrounding code
  - Can impact surrounding optimizations
  - Can be subject to code motion
- Conditional instrumentation possibly tricky
- Requires source code and compilation

**Source Code Instrumentation**

**Manual**
Programmer inserts measurement code into locations of interest.
- Fine grained placement control
- Tedious and possibly error prone

**Assisted**
Tool inserts measurement code into specified locations.
- Tool guarantees systematic coverage
- Specification of locations limited

For tool examples think about logging frameworks or macro processors.

**Source Code Instrumentation Problems**

**Configurability**
We want to have simple way to turn instrumentation on and off.
- Preprocessing
- Conditional calls

Think what a modern runtime will do with the following:

```java
log.debug ("App_results_are_'" + results.toString () + ".");
log.debug ("App_results_are_('{}', results);
if (log.isDebugEnabled ()) {
  log.debug ("App_results_are_'" + results.toString () + ".");
}
```

**Reliability**
We need reliable association between instrumentation and application code.

Think what a modern compiler will do with the following:

```java
int sqrt_counter = 0;
inline double counted_sqrt (double x) {
```
sqrt_counter ++;
return (sqrt (x));
}

This is the square root function disassembly:

```assembly
sqrt:    pxor        xmm1,xmm1    ; Set xmm1 to zero
         ucomisd     xmm1,xmm0     ; Compare argument to zero
         ja          fail         ; Negative argument check
         sqrtsd      xmm0,xmm0     ; Compute square root
         ret          ; Register passing
```

3 Bytecode Instrumentation

**Bytecode Instrumentation**

**Benefits**
- Still relatively easy to insert
- Bytecode contains much metadata
- Compilation produces predictable bytecode
- Program state still naturally available
- Can be done at runtime without sources

**Challenges**
- Requires tools
- Not all languages and environments have bytecode
- Locations in bytecode possibly different from code structure

For tool examples consider ASM or DiSL.
Also aspect oriented frameworks such as AspectJ.

**ASM**

Library for bytecode manipulation.
Main features of ASM are:
- Core API based on visitor design pattern
  - ClassReader to generate events from class file
  - ClassWriter to generate class file from events
  - Transformations implemented as event pipes
  - Adapters for predefined transformations
- Tree API for in memory class file representation
  - Can build representation from Core API events
  - Can generate Core API events from representation

[http://asm.ow2.io](http://asm.ow2.io)

**Aspect Oriented Programming**

**Idea**
What if we could express independent concerns by separate code fragments?
- Logging
- Transactions
- Authorization

*concern* Program feature that stands apart from other features.
*join point* Program location where concern code resides.
*pointcut* Specification of a set of join points.
*advice* Code inserted at pointcut.
weave  Insert advice.
Obviously AOP can be used to insert measurement instrumentation.
Some pointcut specifications can introduce significant perturbation.

AspectJ

Aspect oriented programming framework for Java.

Main features of AspectJ are:

- Byte code instrumentation at compile time and load time
- Declarative language for defining instrumentation points
- Instrumenting code written in Java

http://www.eclipse.org/aspectj

Instrumentation with AspectJ

```
aspect Measurement {

    // Select all executions of methods of class Main.
    pointcut allMainMethods (): execute (* Main.* (..));

    // Attach an around advice that measures time.
    Object around (): allMainMethods () {
        long timeBefore = System.nanoTime ();
        Object result = proceed ();
        long timeAfter = System.nanoTime ();
        System.out.println (timeAfter - timeBefore);
        return (result);
    }
}
```

AspectJ Join Points

Join points are:

- call and execution of a method or a constructor,
- execution of an exception handler,
- execution of a static initializer,
- read or write access to a field,
- execution of an advice.

```
execution (int SomeClass.someMethod (int))
execution (String * .getName (..))
call (AnotherClass.* (String))
call (new (long))
handler (RemoteException+)
get (int *.counter)
```

Join points can be further constrained by:

- presence of an annotation,
- location within a class or a method,
- actual type of the current object, called object, arguments,
- control flow selected by particular pointcut,
- boolean expression.

```
this (SomeClass)
target (AnotherClass)
args (int, int, int, int)
cflow (SomePointcut)
within (SomeClass)
```
**AspectJ Pointcuts**

Pointcuts combine specifications of join points using standard operators `&&`, `||`, `!`.

```java
pointcut callToSomeClassFromMain ():
    within (Main) && target (SomeClass+);

pointcut nonRecursiveCallToSomeClass ():
    call (* SomeClass.. ...) && !within (SomeClass)

Pointcuts can make accessible variables in their context:
- current object,
- target object,
- arguments.

```java
pointcut callToSomeClass (SomeClass o):
    call (* SomeClass.. ...) && target (o);

pointcut namingSomething (String name):
    call (void .*setName (String)) && args (name);
```

**AspectJ Advice**

Advice can be associated with join point:
- before the join point,
- after the join point
  - when it returns normally,
  - when it throws an exception,
- around the join point.

```java
before SomePointcut ():
    Object [] arguments = thisJoinPoint.getArgs ();
    for (Object argument : arguments) {
        System.out.println (argument);
    }

Object around AnotherPointcut ():
    return (proceed ());
```

**More AspectJ Features**

Aspects can include declarations across types:
- declare new fields,
- declare new methods,
- declare new constructors,
- introduce new parents,
- introduce new interfaces.

```java
private interface HasCounter {}

declare parents:
    (SomeClass || AnotherClass) implements HasCounter;
private long HasCounter.executionCount = 0;
before (HasCounter o):
    execution (* *.. (...) ) && this (o) {
        o.executionCount ++;
    }
```

**Bytecode Instrumentation Problems**

5
Consider
Inserted instrumentation executes in the same virtual machine as program.

Can this cause any problems?
- Deadlock between analysis and application
- State corruption inside application code
- Arbitrary assumptions in virtual machine
- Bytecode verification failures
- Shared reference handlers
- Coverage approximation
- ...

Program State Corruption

Coverage
Analyses may require total code coverage:
- Memory allocation tracking (leaves important)
- Taint tracking (and any other data flow)
- Reliable race detection
- ...

What happens if we try to instrument every class of the application?
This includes Object, String, System classes.
These will likely be used by instrumentation and analysis code too.
It is (too) easy to run into infinite recursion or state corruption problems.

Dynamic Bypass Pseudocode

```java
static boolean instrumentationOnline = false;

// Instrumentation snippet
if (!instrumentationOnline) {
    instrumentationOnline = true;

    // Actual instrumentation here
    instrumentationOnline = false;
}
```

Simple with single-threaded programs, can be tricky with multiple threads.

DiSL
A bytecode instrumentation framework with emphasis on coverage.
- Language and framework for Java bytecode instrumentation
- Similar to aspects, but read only and with more control
- Allows to write instrumentation snippets directly in Java
- Instrumentation points are selected using annotations
- Dynamic bypass is provided automatically

http://disl.ow2.org

Example Instrumentation Snippet

```java
@Before {
    marker = BodyMarker.class,
    scope = "TargetClass.print_(boolean)",

Based on Kell et al.: The JVM is Not Observable ...
```
```java
public static void precondition () {
    System.out.println("Precondition!");
}
```

**snippet** Code inserted as instrumentation.

**marker** Specification of location to instrument.

**scope** Specification of classes to instrument.

**guard** Instrumentation condition.

### DiSL Architecture

**Instrumentation Server**

Standalone server responsible for creating instrumented classes.

- Standalone to minimize perturbation
- Instrumentation using ASM
- Optimizations

**Application Client**

Java virtual machine executing the instrumented application.

- JVMTI agent to intercept class loading process
- Remote communication with instrumentation server
- Also executes whatever instrumentation code is inserted

### More DiSL Examples

Look at the examples from the DiSL distribution. Use the `ant run` command to execute individual examples.

**smoke** A minimum example demonstrating the before and after advice on a method.

**local** An example demonstrating the use of a synthetic local variable.

**scope** Limiting instrumentation scope.

**marker** Implementing custom marker.

**guard** Using guards to restrict instrumentation.

**static** Using and implementing static context.

**dynamic** Using dynamic context.

## 4 Machine Code Instrumentation

### Machine Code Instrumentation

**Benefits**

- Machine code (almost) always available
- Looking at code in very fine resolution

**Challenges**

- Machine code difficult to analyze
  - Mixing code and data
  - Variable length instructions
  - Very far from source code structure
- Inserting extra code difficult
  - No space for extra instructions
  - Register state must be preserved
- Some patterns complicate things
  - Auto generated or self modifying code
  - Computed branch targets

### Recognizing Machine Code
DUMP

... 04 0A 11 1F 11 11 ...

AS CODE

... 04 0A add $0xa,%al
11 1F adc %ebx,(%rdi)
11 11 adc %edx,(%rcx)
...

AS BITS

Shifting Machine Code

BEFORE PATCH

8A 02  mov (%rdx),%al
84 C0  test %al,%al
74 05  je loop_exit
48 FF C2  inc %rdx
EB F5  jmp loop_head
...

AFTER PATCH

8A 02  mov (%rdx),%al
EB 01 02 03 04  callq probe
84 C0  test %al,%al
74 05  je loop_exit
48 FF C2  inc %rdx
EB F5  jmp loop_head
...

Machine Code Instrumentation

Available tools use combinations of many techniques:

- Overwrite instrumentation locations
- Instrument only prepared locations
- Use dynamic instrumentation

Example tools: DTrace, KProbes, PIN, Valgrind, DynamoRIO.

5 Instrumentation Overwriting Code

Overwriting Instructions

Instrumentation can be inserted by overwriting the instruction(s) at the target location.

Challenges

- Must overwrite only single location
  - As little as single byte on variable opcode length architectures
  - Single instruction on constant opcode length architectures
- Overwrite must be an atomic operation
- Original instruction must be replayed
- Specialized instructions
Intel INT 3 opcode is single byte \(0xCC\)
- Translates into SIGTRAP on Linux
- But also writes on stack
- Hardware support
- Explicit control transfers or barriers sometimes needed
- Trampolines

**Instrument Prepared Locations**

Instrumentation can be inserted at locations that were previously prepared for such use.

**Challenges**

- Identifying suitable locations
- Low overhead when not instrumented
- Prologues
  - Compilers can generate suitable function prologue
- Exported symbols
  - Reasonable location to expect instrumentation at
  - Often called through relatively standard code (PLT)
- Specialized instructions
  - Intel NOP has opcode variants for up to nine bytes
  - Atomic updates for long variants require some care

**Linux Kernel Function Tracer**

System for tracing statically instrumented function calls (and several other metrics) in kernel:

- Instrumentation code inserted by compiler /sys/kernel/debug/tracing/available_filter_functions
- Probes dynamically disabled and enabled
- Per processor buffer for event traces /sys/kernel/debug/tracing/trace
- Controlled through debug file system /sys/kernel/debug/tracing/current_tracer

**Kernel Function Tracer Details**

The kernel function tracer requires compiler support. When the kernel configuration includes the FTRACE infrastructure, the -pg -mfentry command line options are included among the compiler arguments. This option, originally intended for profiling, tells GCC to insert a call to a profiling probe at the start of each function. The kernel uses this call to produce function execution traces.

To minimize overhead, the kernel replaces all calls to the profiling probe with NOP instructions at boot time.

When tracing is enabled, probes are inserted in place of the NOP instructions.

To play with the function tracer and other tracing modules, try:

```
cd /sys/kernel/debug/tracing
# See what tracers are available.
cat available_tracers
# Enable the function tracer and see the output.
echo function > current_tracer
cat trace
# Constrain the function trace to only trace particular function.
echo do_syscall_64 > set_ftrace_filter
cat trace
# Enable the function graph tracer and see the output.
echo do_syscall_64 > set_graph_function
echo function_graph > current_tracer
```

\(^1\)See Chamith et al.: Living On The Edge … doi:10.1145/2908080.2908084
\(^2\)See/usr/src/linux/Documentation/trace/ftrace.txt
cat trace

# Pause and resume the current tracer.
echo 0 > tracing_on
echo 1 > tracing_on

# Disable the current tracer.
echo nop > current_tracer

Note that tracing is disabled while the trace file is being read. This makes sense but means the tail command does not show continuous tracing output.

The kernel function tracer can also be controlled through the perf tool.

To see how the function entry point is modified for tracing, install the kernel symbol information and disassemble the live kernel using the crash tool.

This is the output of dis do_sys_open with tracing disabled:

```
crash> dis do_sys_open
0xffffffff99315e00 <do_sys_open>:       nopl 0x0(%rax,%rax,1) [FTRACE NOP]
0xffffffff99315e05 <do_sys_open+5>:      push %r15
0xffffffff99315e07 <do_sys_open+7>:      and $0xffff,%cx
0xffffffff99315e0c <do_sys_open+12>:     push %r14
0xffffffff99315e0e <do_sys_open+14>:     or $0x8000,%cx
0xffffffff99315e13 <do_sys_open+19>:     push %r13
0xffffffff99315e15 <do_sys_open+21>:     push %r12
...
```

The same with tracing enabled:

```
crash> dis do_sys_open
0xffffffff99315e00 <do_sys_open>:      callq 0xffffffffc0ee1000
0xffffffff99315e05 <do_sys_open+5>:    push %r15
0xffffffff99315e07 <do_sys_open+7>:    and $0xffff,%cx
0xffffffff99315e0c <do_sys_open+12>:   push %r14
0xffffffff99315e0e <do_sys_open+14>:   or $0x8000,%cx
0xffffffff99315e13 <do_sys_open+19>:   push %r13
0xffffffff99315e15 <do_sys_open+21>:   push %r12
...
```

Remember to exit the tool between changes to see the updates.

---

**Linux Kernel Probes**

Interfaces that allow to instrument:

- Any single instruction in kernel (Kprobes)
- Any function entry in kernel (Jprobes) deprecated in favor of function tracer
- Any function exit in kernel (Return Probes)

---

**Kprobes**

Replace target instruction with breakpoint instruction

- Breakpoint instruction is single byte
- Control transfer similar to interrupt
- Jumps can also be used (faster)

Execute probe code

- Registers saved as in other interrupts
- Handler for both pre code and post code

---

*See /usr/src/linux/Documentation/kprobes.txt*
Single step the replaced instruction
- Must be done inside interrupt handler
- Requires understanding all instructions

**Jprobes**

Replace function entry with Kprobe
- Kprobe saves register state and (part of) stack state (because compiler can generate Jprobe code that modifies it)
- Kprobe modifies handler return address to point to Jprobe

Execute probe code
- Jprobe executes as if it were the called function
- On return control is passed to probe exit handler

Restore context on probe exit
- Copy back content saved by Kprobe
- Resume execution of probed function

**Return Probes**

Replace function entry with Kprobe
- Kprobe saves original return address (limited memory here)
- Kprobe modifies function return address to point to trampoline
- Trampoline is instrumented with another Kprobe at system boot time

Execute function code
- Function executes normally
- On return control is passed to trampoline Kprobe

**Linux User Mode Probes**

System for tracing dynamically instrumented user mode code locations:
- Instrumentation code inserted by kernel on code load
- Controlled through debug file system /sys/kernel/debug/tracing/uprobe_events echo "<type> <file>:<offset> [arglist]

**Linux User Mode Probe Details**


```
# List what functions are available for probing.
perf probe -x basic -F

# List what lines are available for probing within a function.
perf probe -x basic -L main

# List what variables are available for probing on a line within a function.
perf probe -x basic -V main:13

# Set a user mode probe on a line and include variable content in event record.
perf probe -x basic -L main:13 i primes

Once the probe is set, in can be used as any other trace point, for example with other perf commands. It can also be examined directly in the kernel tracing infrastructure.

# See how the probe was defined in the debug file system.
cat /sys/kernel/debug/tracing/uprobe_events

# Enable the probe tracing event and observe the trace and the profile.
echo 1 > /sys/kernel/debug/tracing/events/probe_basic/main_L13/enable
timeout 1 ./basic
```

*See /usr/src/linux/Documentation/trace/uprobetracer.txt*
cat /sys/kernel/debug/tracing/trace

cat /sys/kernel/debug/tracing/uprobe_profile

To see how the probe point is modified, keep the probe enabled and compare file disassembly with live code disassembly:

# File disassembly. Does not show the probe.
objdump --disassemble=main --source basic

```
...
// Any number that is still marked
// as potentially prime is prime.
if (can_be_prime [i]) {
  4010cd: 80 ba 80 41 40 00 00 cmpb $0x0,0x404180(%rdx)
  4010d4: 74 ea je 4010c0 <main+0x20>
...
```

# Live code disassembly. Shows the probe.
./basic & gdb -ex “disassemble /rs_main” basic $!

```
...
21 // Any number that is still marked
22 // as potentially prime is prime.
23 if (can_be_prime [i]) {
   0x00000000004010cd <+45>: cc int3
   0x00000000004010ce <+46>: ba 80 41 40 00 mov $0x404180,%edx
   0x00000000004010d3 <+51>: 00 74 ea 8d add %dh,-0x73(%rdx,%rbp,8)
...
```

Note how the disassembly is confused by the fact that the seven byte cmp instruction is replaced with the one byte int instruction. The disassembler considers the leftover part of the cmp instruction opcode to be the opcode of the next instruction after int. This is what the processor would also do if the execution resumed immediately after the int instruction. The probe handler must therefore adjust the return address after executing the original cmp instruction. Essentially, this is done by single stepping the original instruction copied to a different location, details are available in kernel sources in /arch/x86/kernel/uprobes.c.

---

**Linux Extended Berkeley Packet Filters**

Framework for securely injecting code into kernel.

**Code**

Injected code written in limited bytecode:

- RISC style instructions
- Limit on instruction count (1M)
- Limit on branching (no loops)
- Static memory access checks

Bytecode supported by LLVM backend.

**Maps**

Data export through maps:

- In kernel key value stores
- Both global and per processor

---

More bpf Examples

Examine the bpftrace examples from [https://github.com/iovisor/bpftrace](https://github.com/iovisor/bpftrace)

---

6See man bpf
6 Instrumentation Translating Code

Dynamic Instrumentation

Instrumentation can be inserted by translating code during execution.

Challenges

- Identifying code to translate
- Keeping execution overhead reasonably low
- Making translation invisible to application
- Code recognized during execution
  - Anything executed must be code
  - Translate in units of basic blocks
  - Chain basic blocks from hot paths into traces
  - Cache and reuse translations during execution
- Instrument inside basic block discovery notification
- Interface to internal code representation
  - Close to binary form in "Copy and Annotate" (PIN, DynamoRIO)
  - Close to compiler IR in "Disassemble and Resynthesize" (Valgrind)

PIN


- C and C++ API
- Provides multiple instrumentation points such as Routine (RTN), Image (IMG), Instruction (INS)
- Instrumentation snippet is normal C/C++ code
- Operates in JIT mode or probe mode
- Supports x86

PIN Tool Example

```c
int main (int argc, char * argv []) {
  if (PIN_Init (argc, argv)) exit (1);
  INS_AddInstrumentFunction (CountInstruction, 0);
  PIN_StartProgram ();
}

VOID CountInstruction (INS ins, VOID * v) {
  INS_InsertCall (ins, IPOINT_BEFORE, (AFUNPTR) DoCount, IARG_END);
}

VOID DoCount () { ... }
```

... run with pin -t pintool.so -- command

Valgrind

Open source dynamic binary instrumentation tool. http://valgrind.org

- C API
- Compiler style intermediate representation (VEX)
- Instrumentation implemented as VEX manipulation
- Targets heavyweight instrumentation
- Supports x86, ARM, PPC, MIPS ...

Valgrind VEX Example

**Original Instruction**

7Based on code from Intel PIN examples
add eax,ebx

----- IMark(0x123456, 2, 0) ------
# Connects VEX to original code address and length

t3 = GET:I32(8)   # Guest state offset 8 is EAX
t2 = GET:I32(20) # Guest state offset 20 is EBX
t1 = Add32(t3,t2)
PUT(8) = t1

# Does not show flags and program counter updates

Valgrind VEX Example

Original Instruction

add [eax+4],edx

----- IMark(0x123456, 4, 0) ------
# Connects VEX to original code address and length

t3 = Add32(GET:I32(8),0x4:I32) # Non flattened
t2 = LDle:I32(t3) # Little endian load
t1 = GET:I32(16)     # Guest state offset 16 is EDX
t0 = Add32(t2,t1)
STle(t3) = t0        # Little endian store

# Does not show flags and program counter updates

Based on code from Valgrind headers