

Chronicler: Lightweight Recording to Reproduce Field Failures

Jonathan Bell, Nikhil Sarda and Gail Kaiser
Columbia University, New York, NY USA

What happens when software crashes?

A problem has been detected and windows has been shut down to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)

*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory

Physical memory dump complete.

Contact your system administrator or technical support group for further assistance.

You need to restart your computer. Hold down the Power button for several seconds or press the Restart button.

Veillez redémarrer votre ordinateur. Maintenez la touche de démarrage enfoncée pendant plusieurs secondes ou bien appuyez sur le bouton de réinitialisation.

Sie müssen Ihren Computer neu starten. Halten Sie dazu die Einschalttaste einige Sekunden gedrückt oder drücken Sie die Neustart-Taste.

コンピュータを再起動する必要があります。パワーボタンを数秒間押し続けるか、リセットボタンを押してください。



 **Mozilla Crash Reporter** ✕

We're Sorry

Firefox had a problem and crashed. We'll try to restore your tabs and windows when it restarts.

To help us diagnose and fix the problem, you can send us a crash report.

☒ Tell Mozilla about this crash so they can fix it

[Details...](#)

Add a comment (comments are publicly visible)

☒ Include the address of the page I was on

☐ Allow Mozilla to contact me about this report

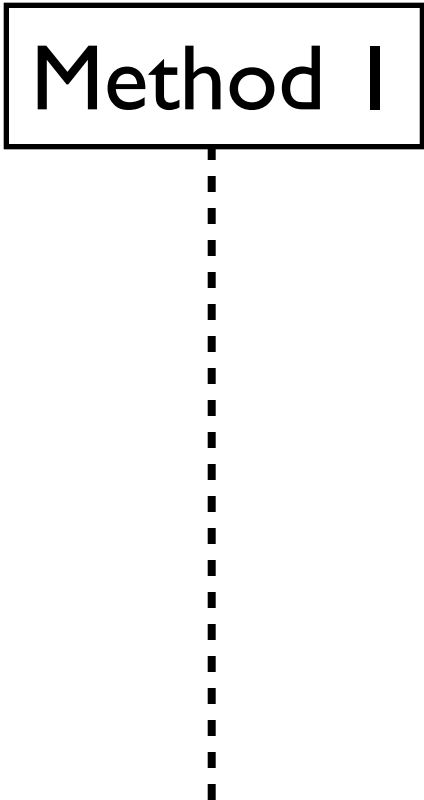
Your crash report will be submitted before you quit or restart.

[Restart Firefox](#) [Quit Firefox](#)

Frame	Module	Signature	Source
0	XUL	js::MaybeGC	js/src/jsgc.cpp:2654
1	XUL	nsJSContext::ScriptEvaluated	dom/base/nsJSEnvironment.cpp:2806
2	XUL	nsCxPusher::~~nsCxPusher	content/base/src/nsContentUtils.cpp:3127
3	XUL	nsGlobalWindow::SetNewDocument	dom/base/nsGlobalWindow.cpp:2150
4	XUL	DocumentViewerImpl::InitInternal	layout/base/nsDocumentViewer.cpp:926
5	XUL	DocumentViewerImpl::Init	layout/base/nsDocumentViewer.cpp:676
6	XUL	nsDocShell::SetupNewViewer	docshell/base/nsDocShell.cpp:8023
7	XUL	nsDocShell::Embed	docshell/base/nsDocShell.cpp:6075
8	XUL	nsDocShell::CreateAboutBlankContentViewer	docshell/base/nsDocShell.cpp:6814
9	XUL	nsDocShell::EnsureContentViewer	docshell/base/nsDocShell.cpp:6697
10	XUL	nsDocShell::GetInterface	docshell/base/nsDocShell.cpp:951
11	XUL	nsGetInterface::operator	obj-firefox/x86_64/xpcom/build/nsIInterfaceRequestorUtils.cpp:19
12	XUL	nsCOMPtr_base::assign_from_helper	obj-firefox/x86_64/xpcom/build/nsCOMPtr.cpp:110
13	XUL	nsGlobalWindow::GetDocument	
14	XUL	XUL@0x673d6d	
15	XUL	XPCConvert::NativeInterface2JSObject	js/xpconnect/src/XPCConvert.cpp:837
16	XUL	XPCConvert::NativeData2JS	js/xpconnect/src/XPCConvert.cpp:319
17	XUL	XPCWrappedNative::CallMethod	js/xpconnect/src/xpcprivate.h:3312
18	XUL	XPC_WN_GetterSetter	js/xpconnect/src/xpcprivate.h:2823
19	XUL	js::InvokeKernel	js/src/jsctxinlines.h:372
20	XUL	js::Invoke	js/src/jsinterp.h:119
21	XUL	js::InvokeGetterOrSetter	js/src/jsinterp.cpp:469
22	XUL	js::Shape::get	js/src/jsscopeinlines.h:296

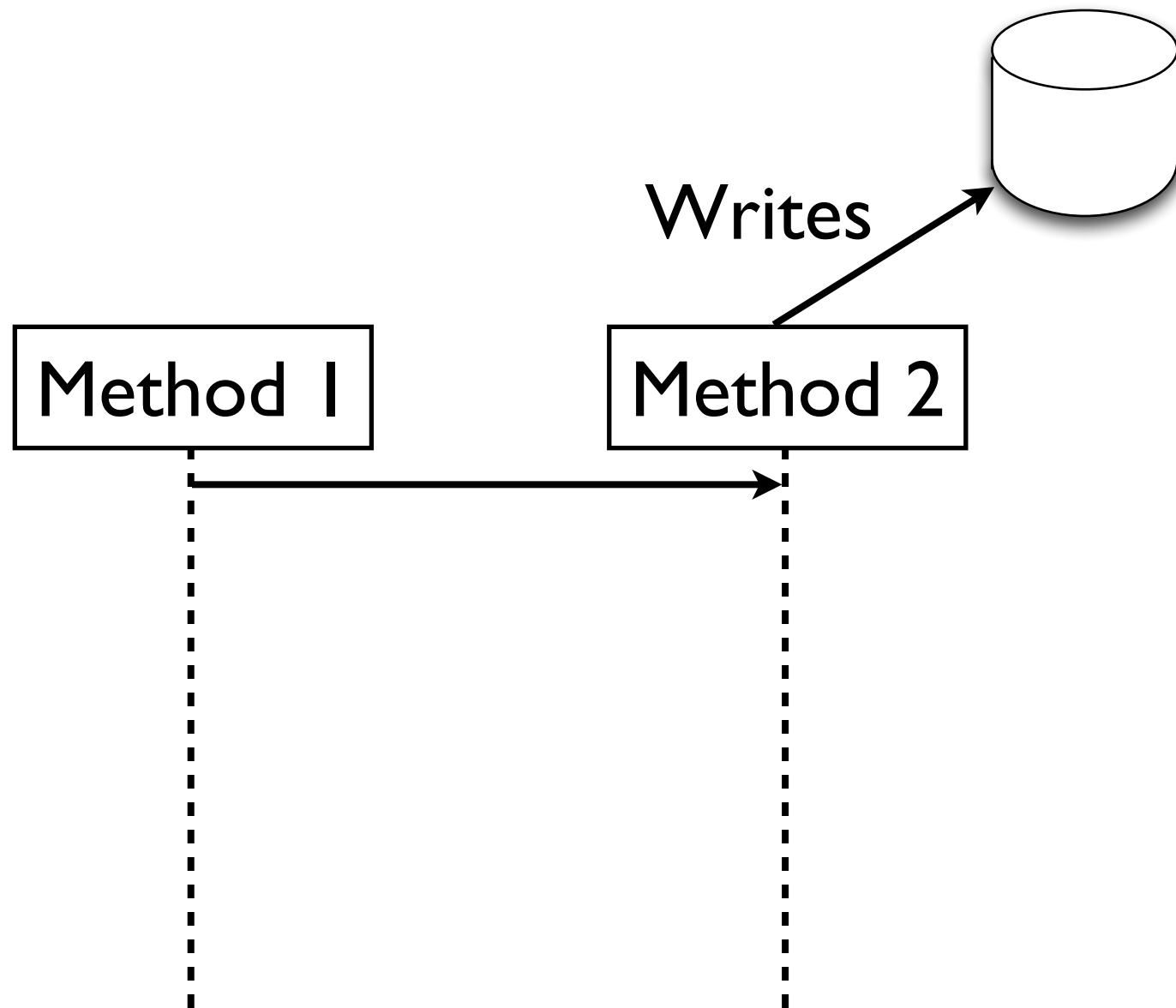
Stack Traces Aren't Enough

Method 1



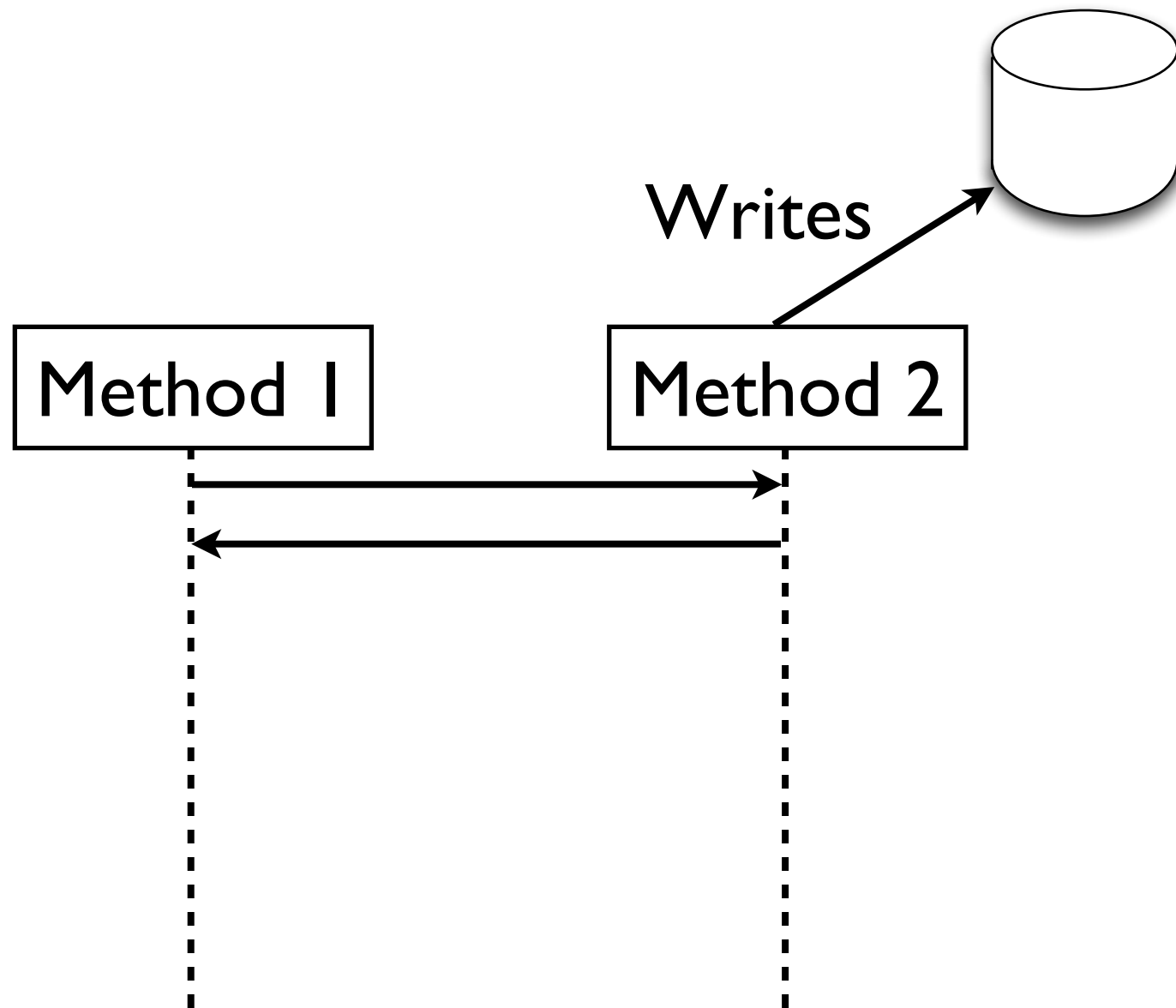
Stack Trace
Method 1

Stack Traces Aren't Enough



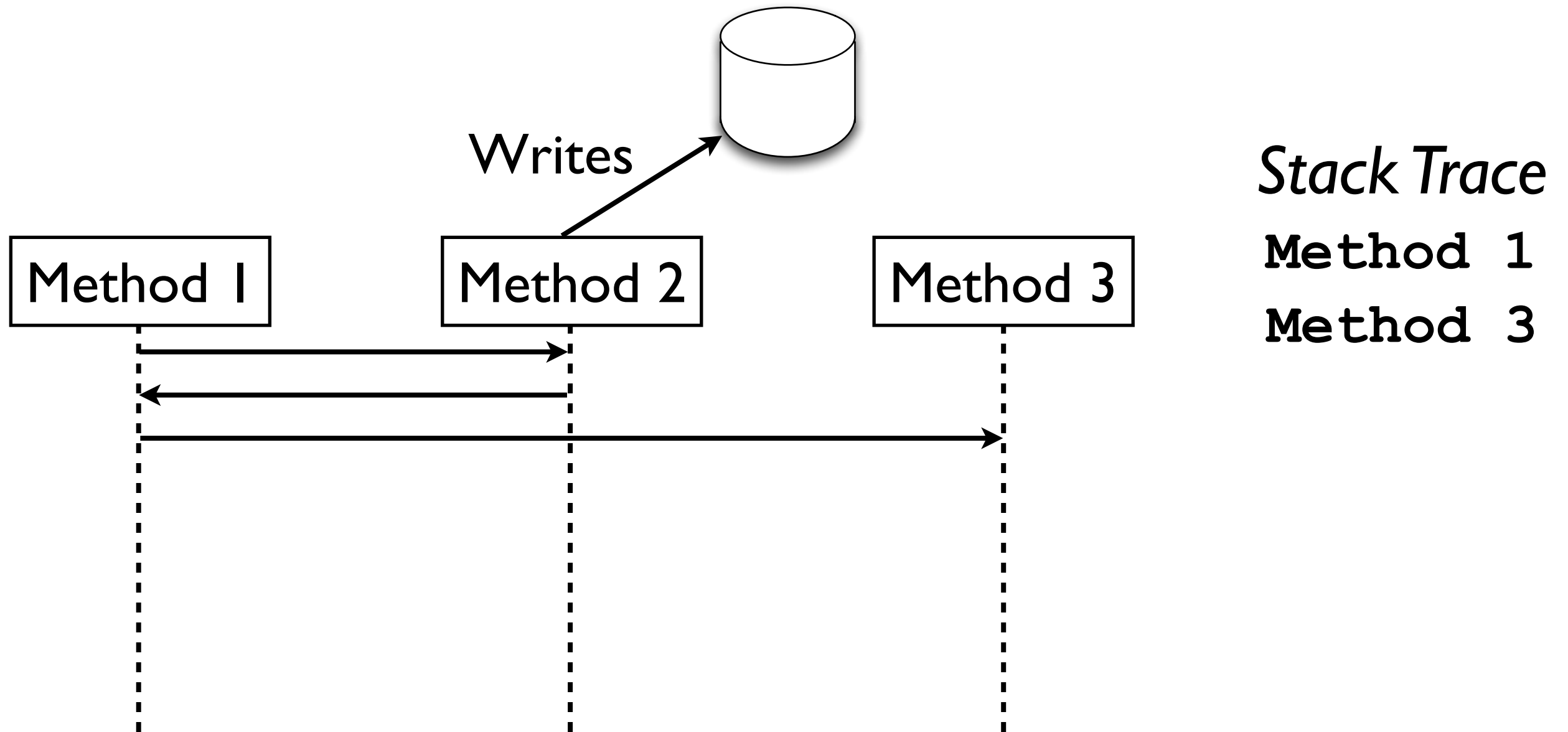
Stack Trace
Method 1
Method 2

Stack Traces Aren't Enough

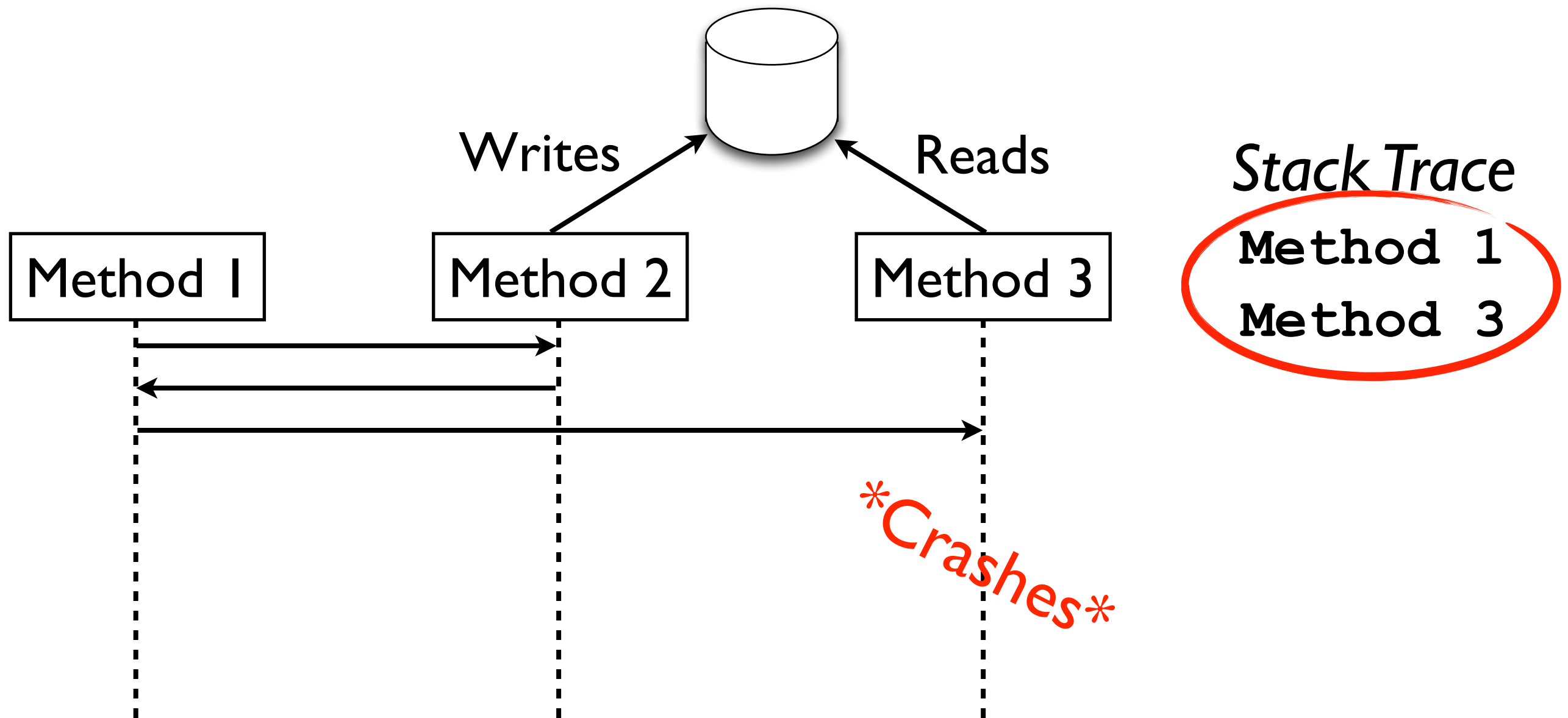


Stack Trace
Method 1

Stack Traces Aren't Enough



Stack Traces Aren't Enough



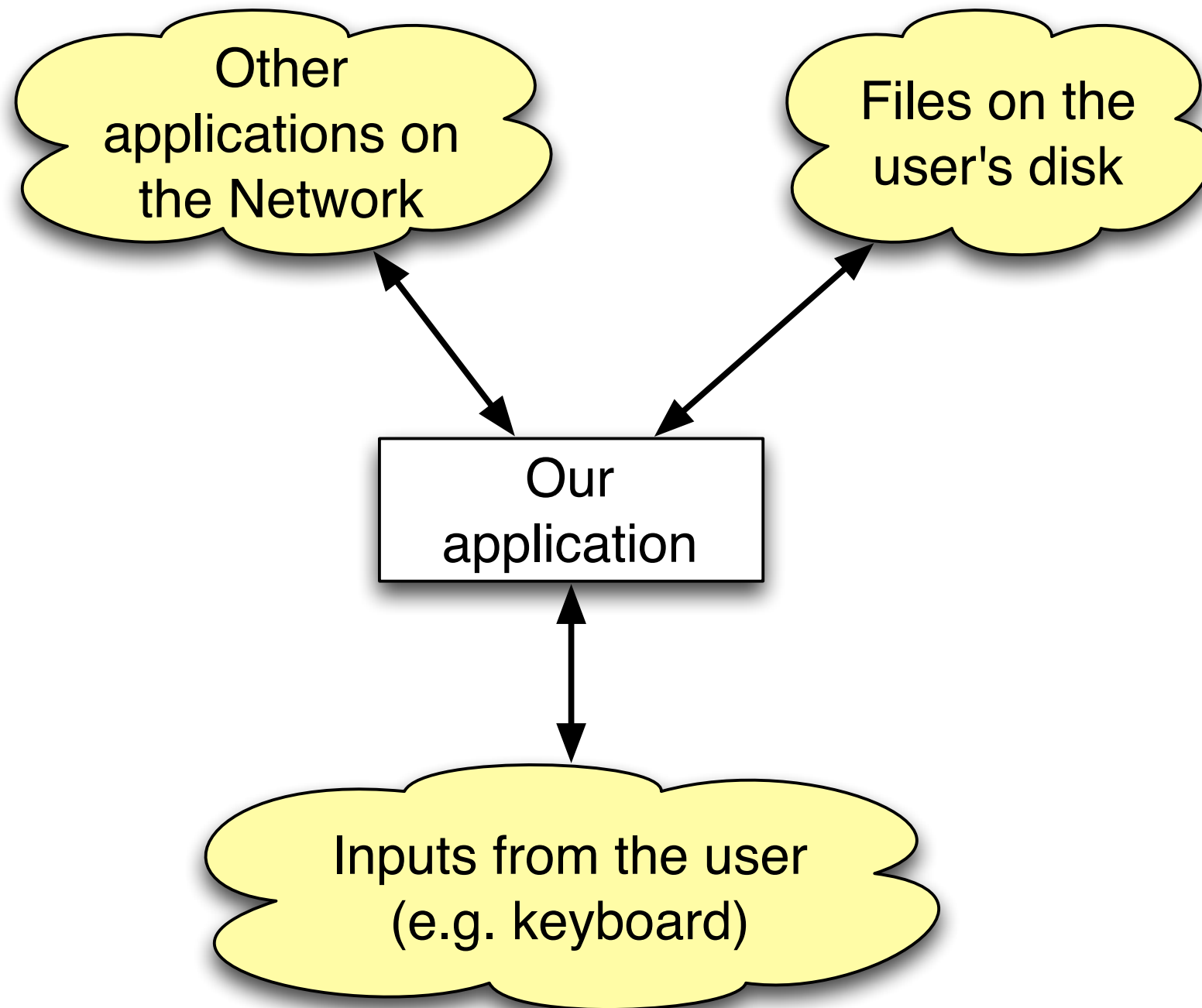
Potential Solutions

- Frequent Snapshots [Artzi et al]
- Guided symbolic execution [Cheung et al], [Crameri et al], [Jin and Orso], [Zamfir and Candea]

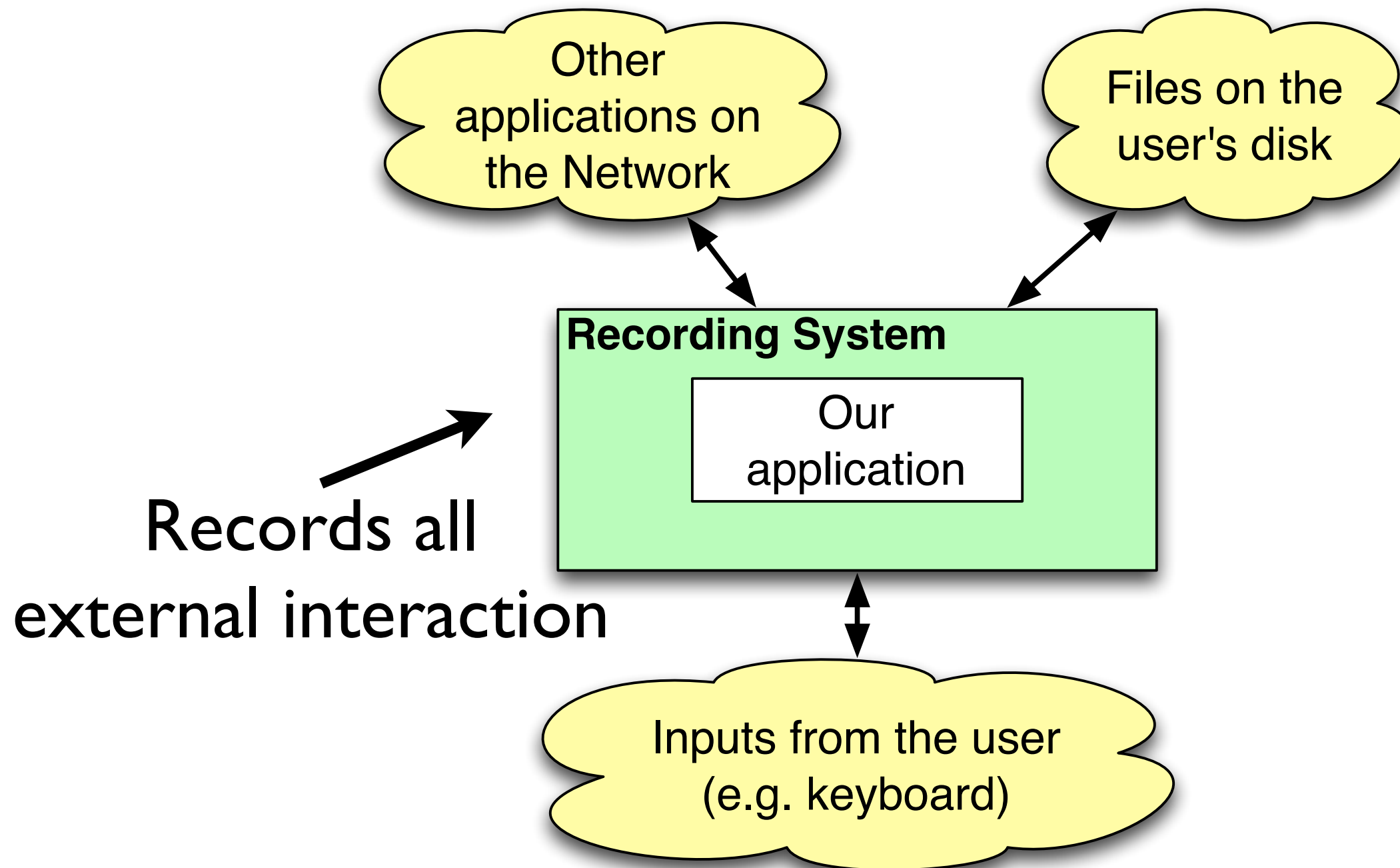
Recording External Inputs

[Geels et al], [Clause and Orso], [Mickens et al], this work

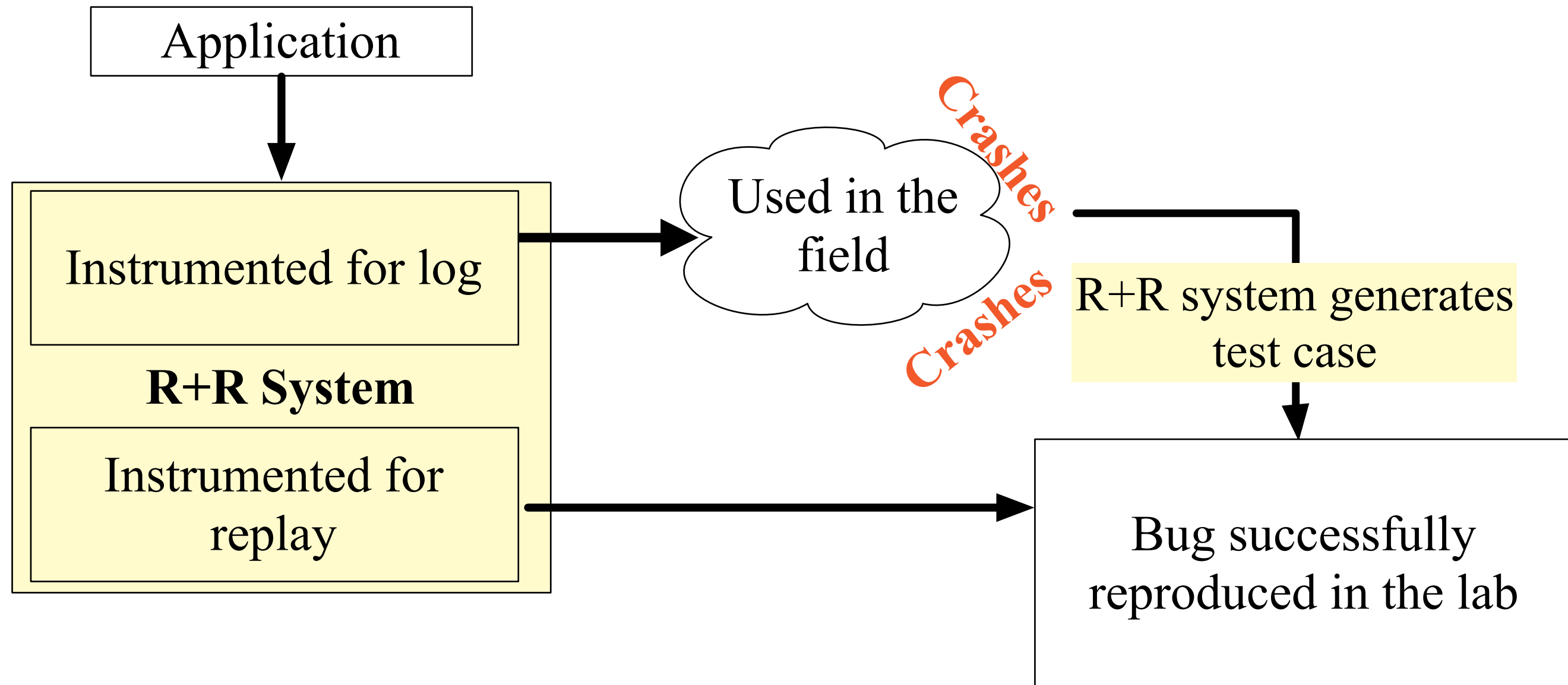
Recording External Inputs



Recording External Inputs



Record and Replay: Workflow



Recording Inputs

- Previous work looks at logging *system calls*
 - e.g. *read, write, open*
- Can lead to very high overhead in VM-based languages, which perform many such operations just to setup the VM!

Our insight: **API** Level Logging

Reading a File: Log System Calls

```
public class ReadFile {  
    public static void main(String[] args) throws  
FileNotFoundException {  
        String text = new Scanner(new  
            File("testFile")).useDelimiter("\\A").next();  
    }  
}
```



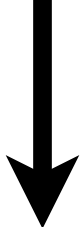
\$ java ReadFile



684 System Calls

Reading a File: API Logging

```
public class ReadFile {  
    public static void main(String[] args) throws  
FileNotFoundException {  
        String text = new Scanner(new  
            File("testFile")).useDelimiter("\\A").next();  
    }  
}
```

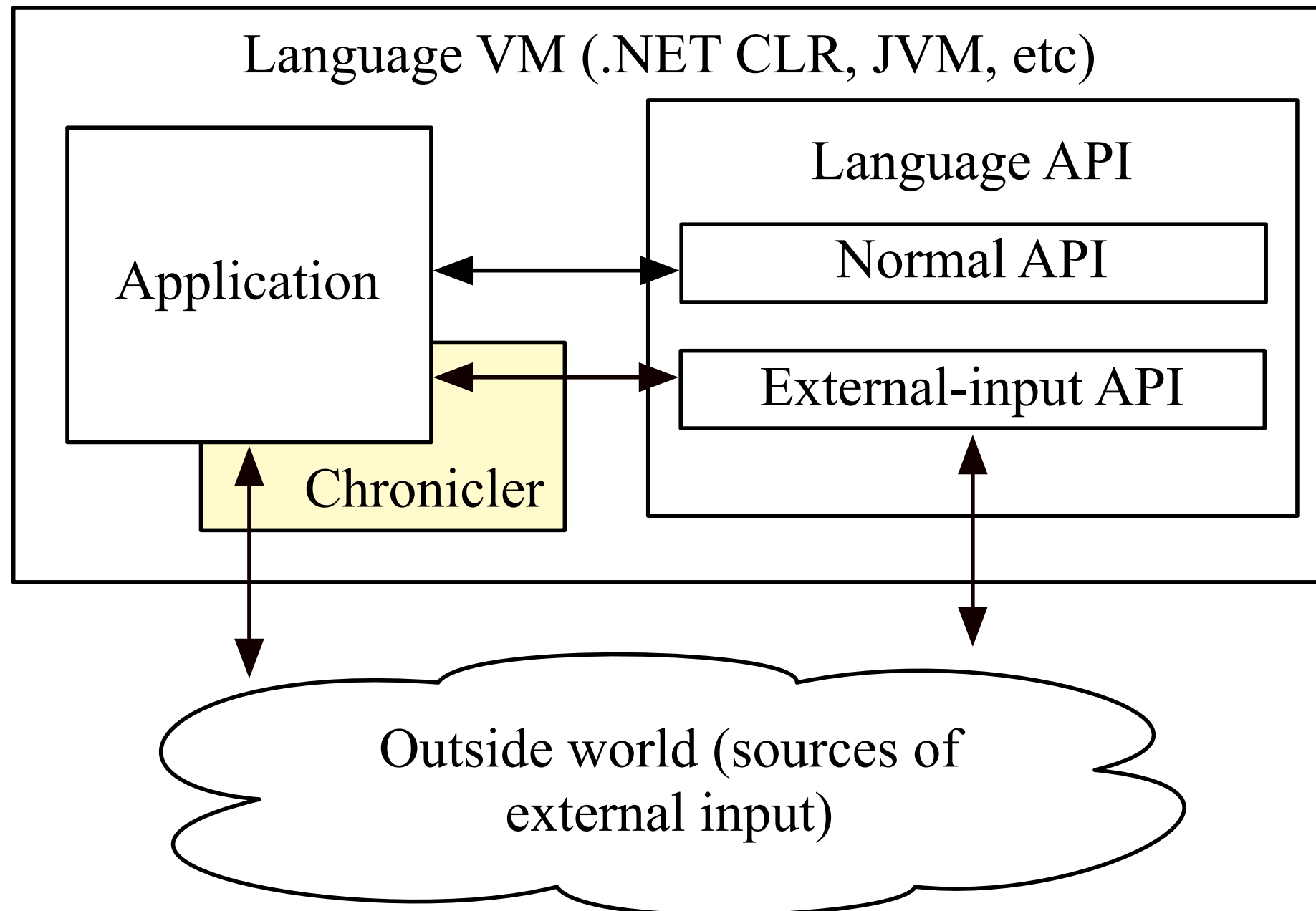


\$ java ReadFile

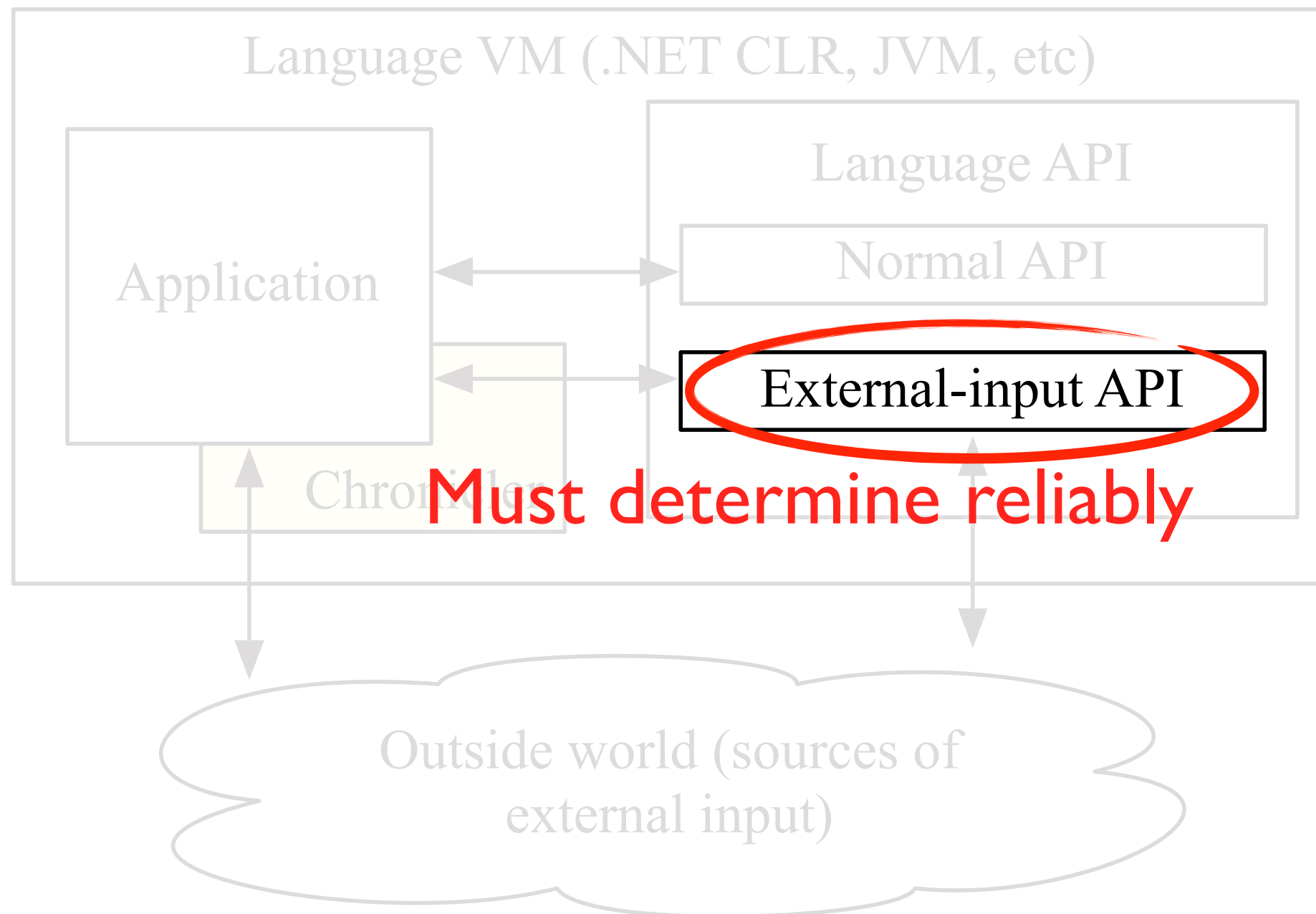


| "External" API call

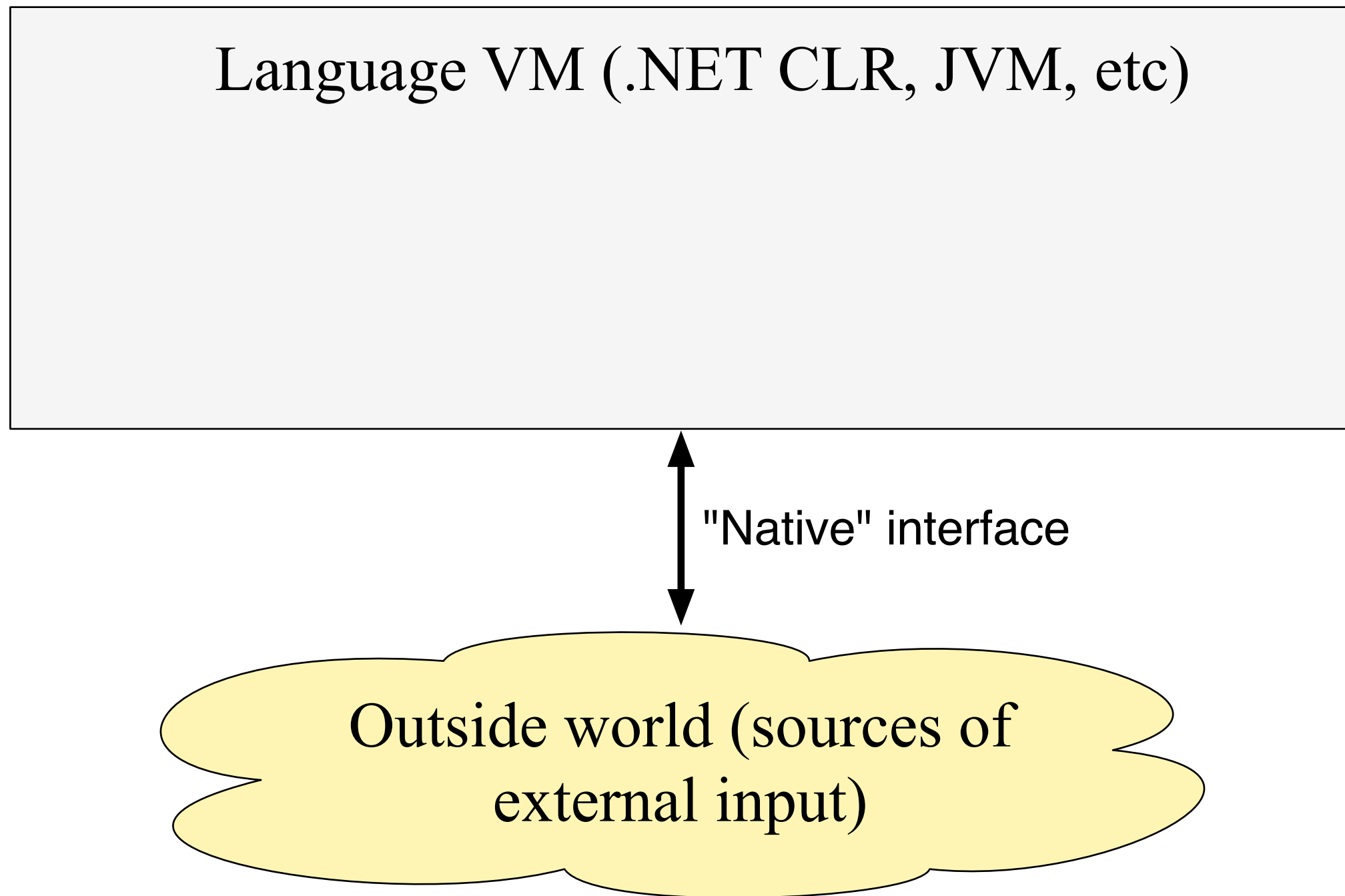
API Level Logging: The Challenge



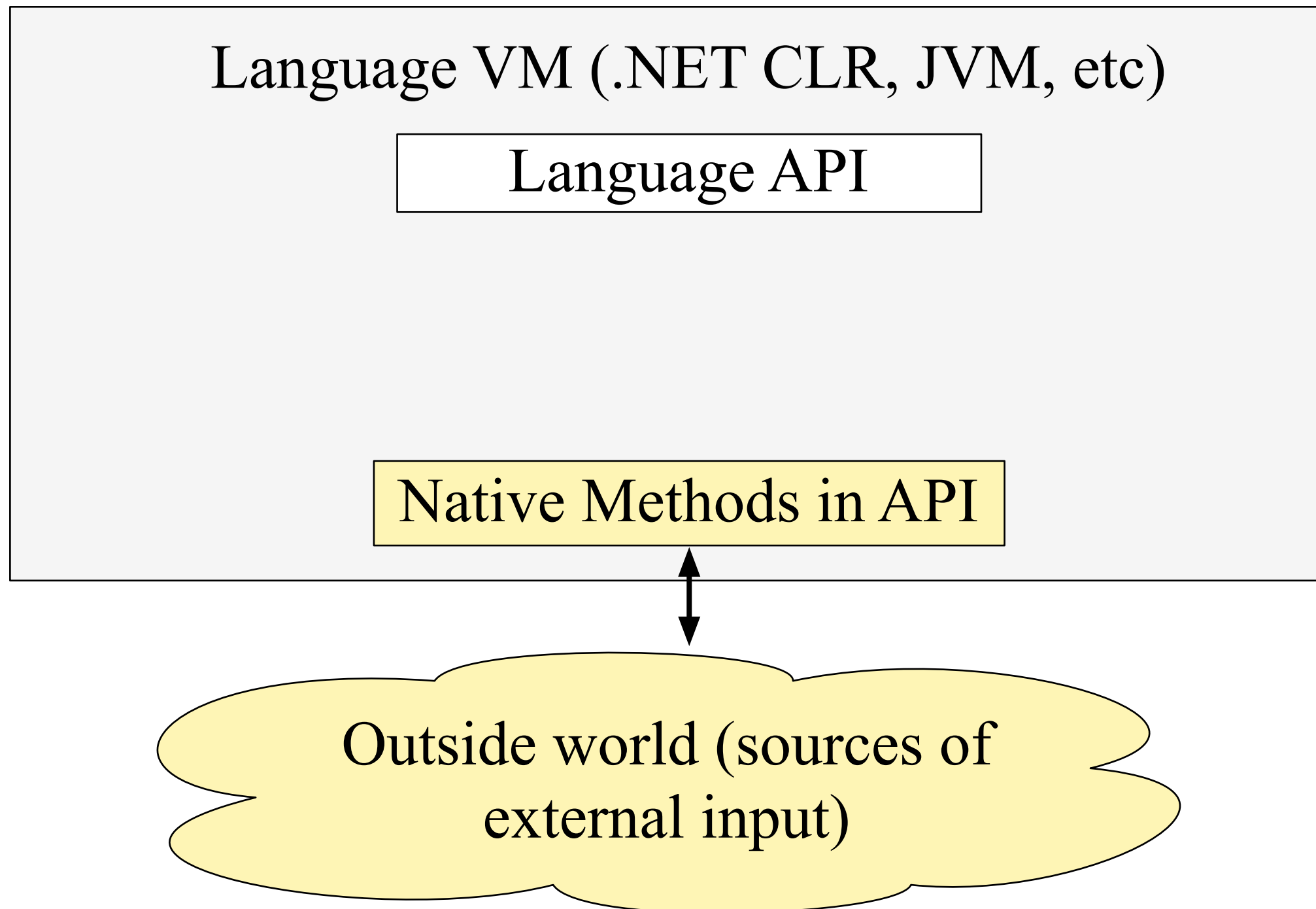
API Level Logging: The Challenge



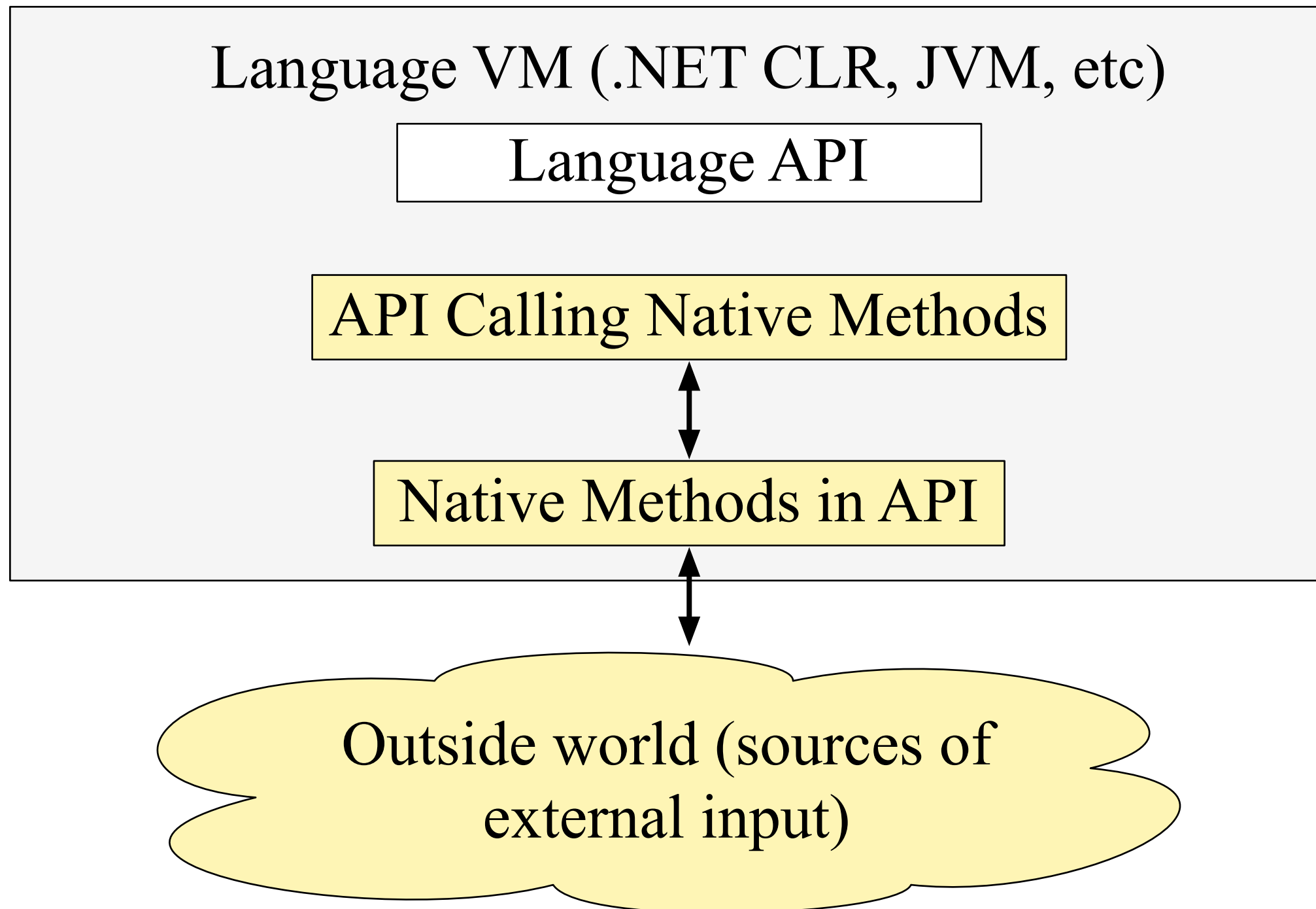
Identifying External Inputs



External Inputs in Java



External Inputs in Java



**Problem: A lot is done
outside of the VM**

Log explosion

Not all native methods return external input

```
public static native void arraycopy ...
```

1984 direct callers

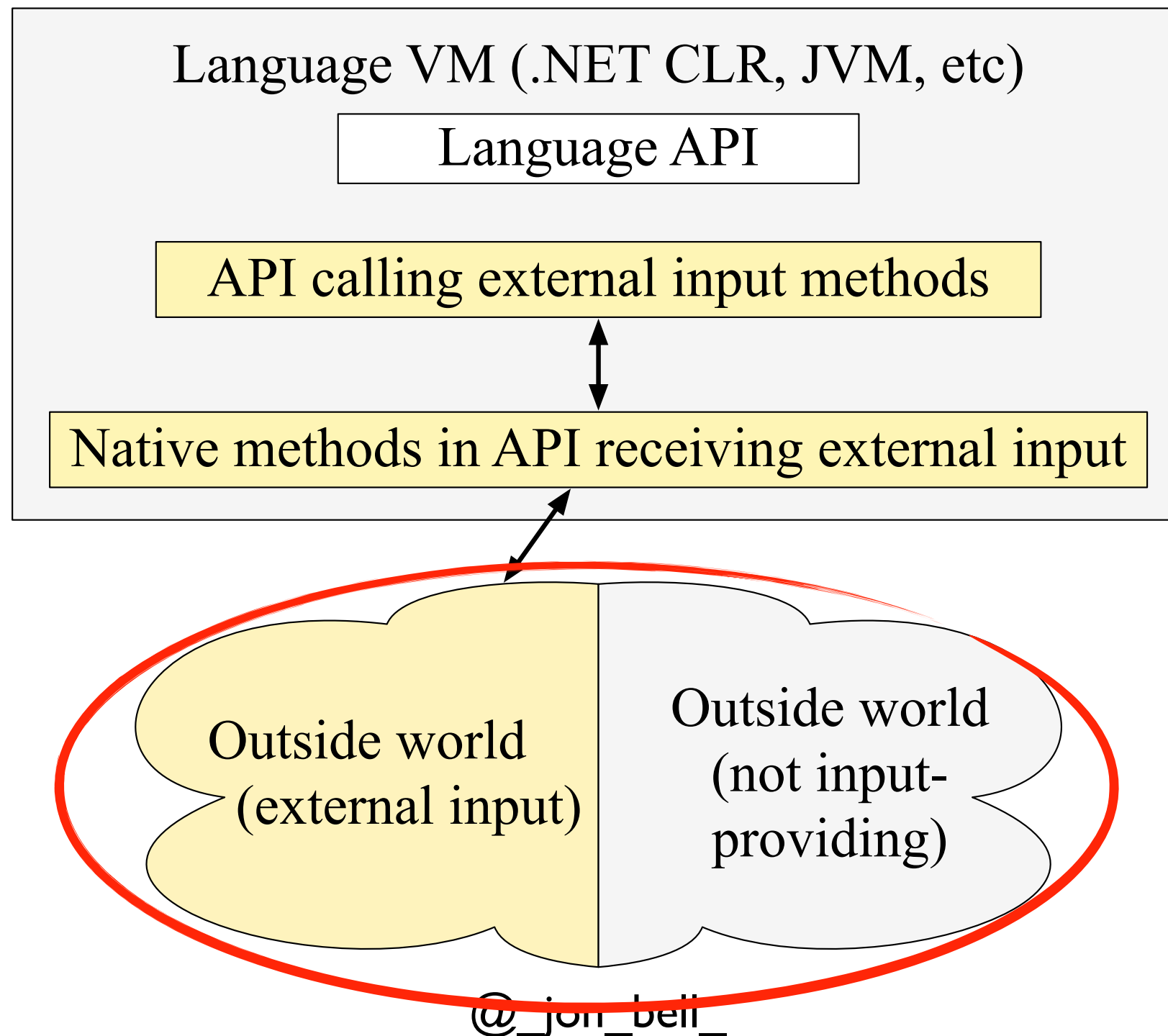
Log explosion: System.arraycopy

```
void getChars(char dst[], int dstBegin) {  
    System.arraycopy(...);  
}
```

```
public String concat(String str) {  
    ...  
    getChars(0, count, buf, 0);  
    ...  
}
```

125,714 indirect callers

Managing Log Explosion



Managing Log Explosion

- Stop list: approx 70 native methods that do NOT gather external input
- Also includes StrictMath, some image processing
- Not necessary to be complete in the stop list

Managing Log Explosion

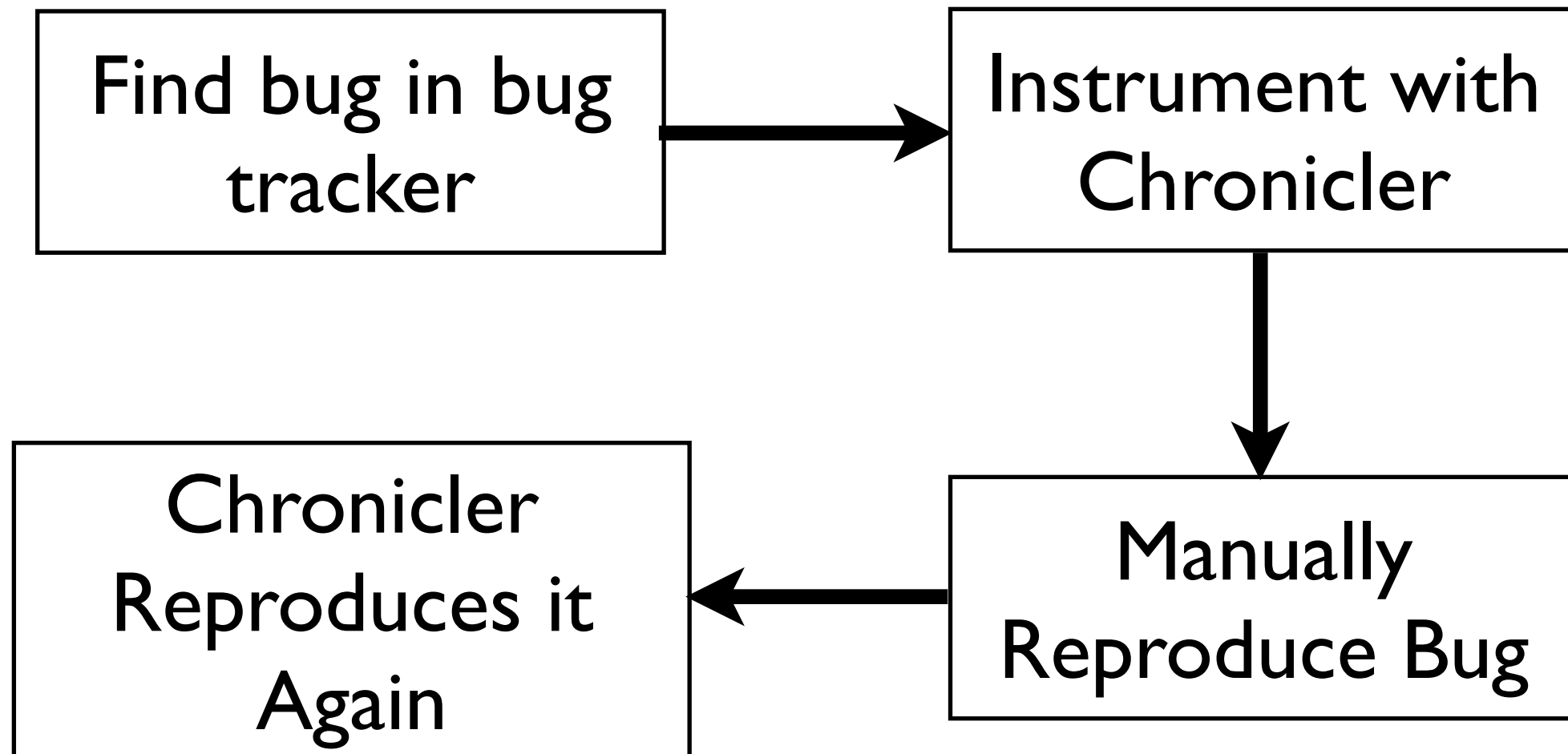
- Stop list: approx 70 native methods that do NOT gather external input
- Also includes StrictMath, some image processing
- Not necessary to be complete in the stop list
- Result: decrease log sites by ~25%

Implementation

- Targets Java
- Bytecode transformation (no source!)
- Logs all external inputs from the API
- Plenty of clever tricks: details in the paper (fast logging, callbacks, finalizers, and more!)

Evaluation

Functionality Evaluation

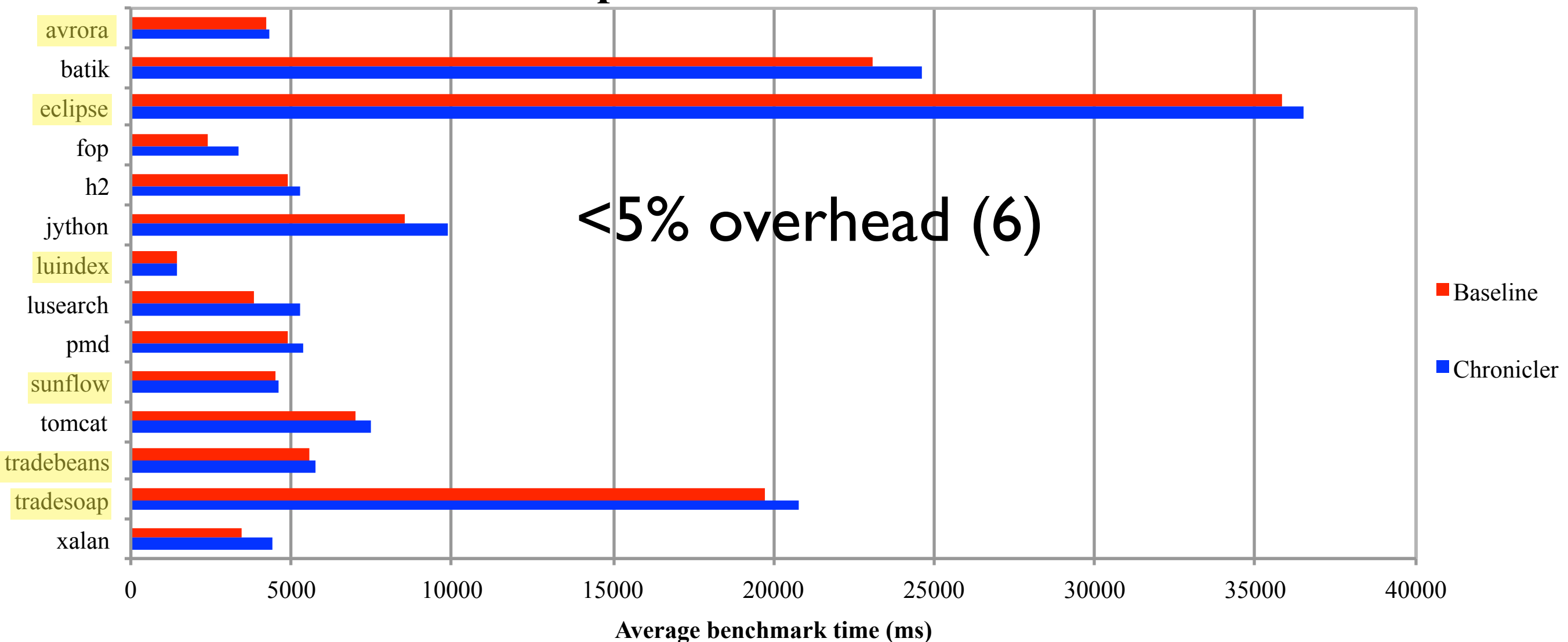


Functionality Evaluation

- Attempted to reproduce 11 real bugs in:
 - Jetty
 - Apache Commons-Math
 - Apache Commons-Lang
 - Groovy
- Succeeded in all cases

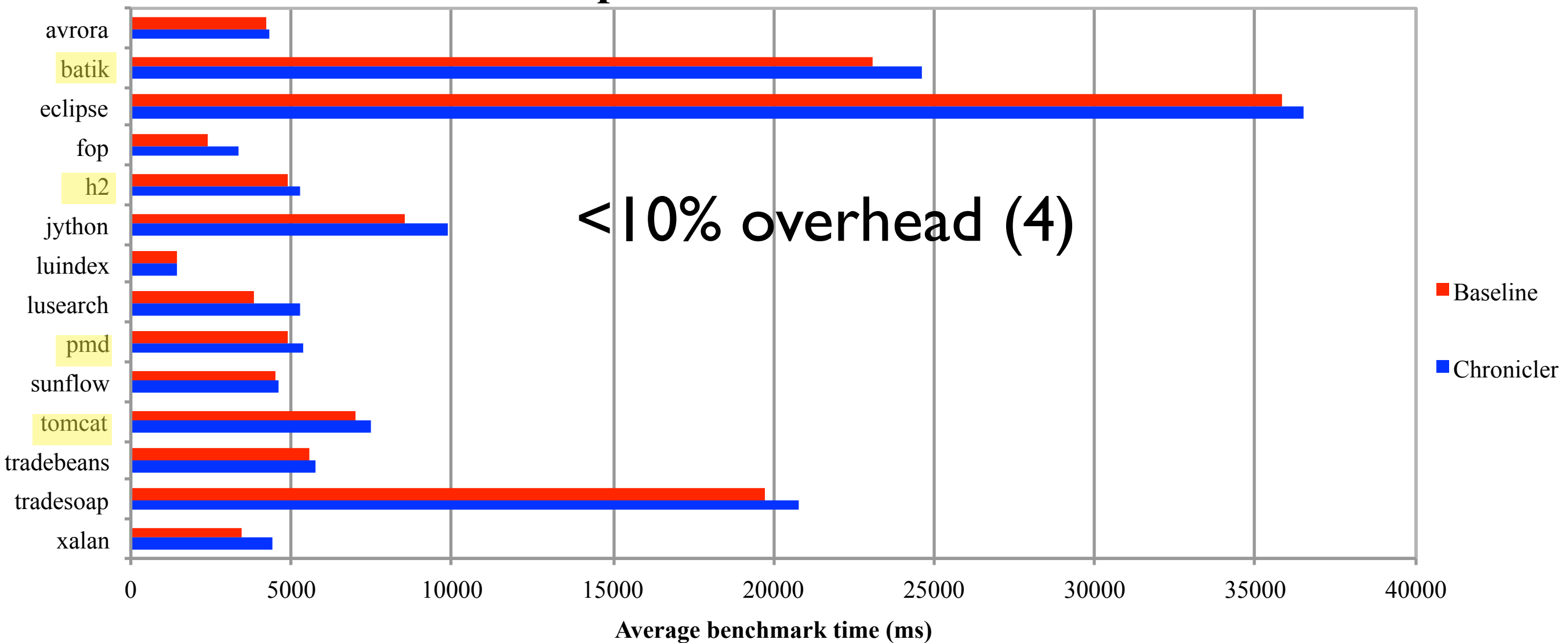
Performance: DaCapo

DaCapo Absolute Performance



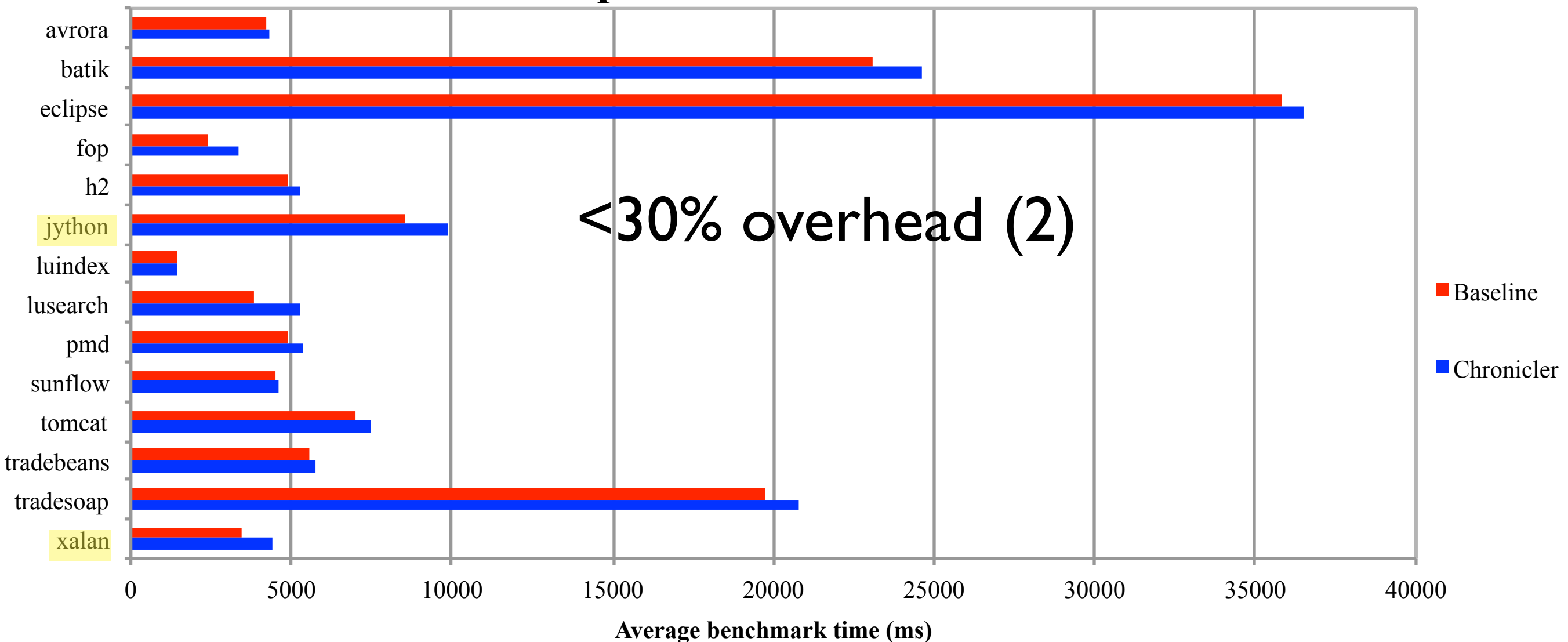
Performance: DaCapo

DaCapo Absolute Performance



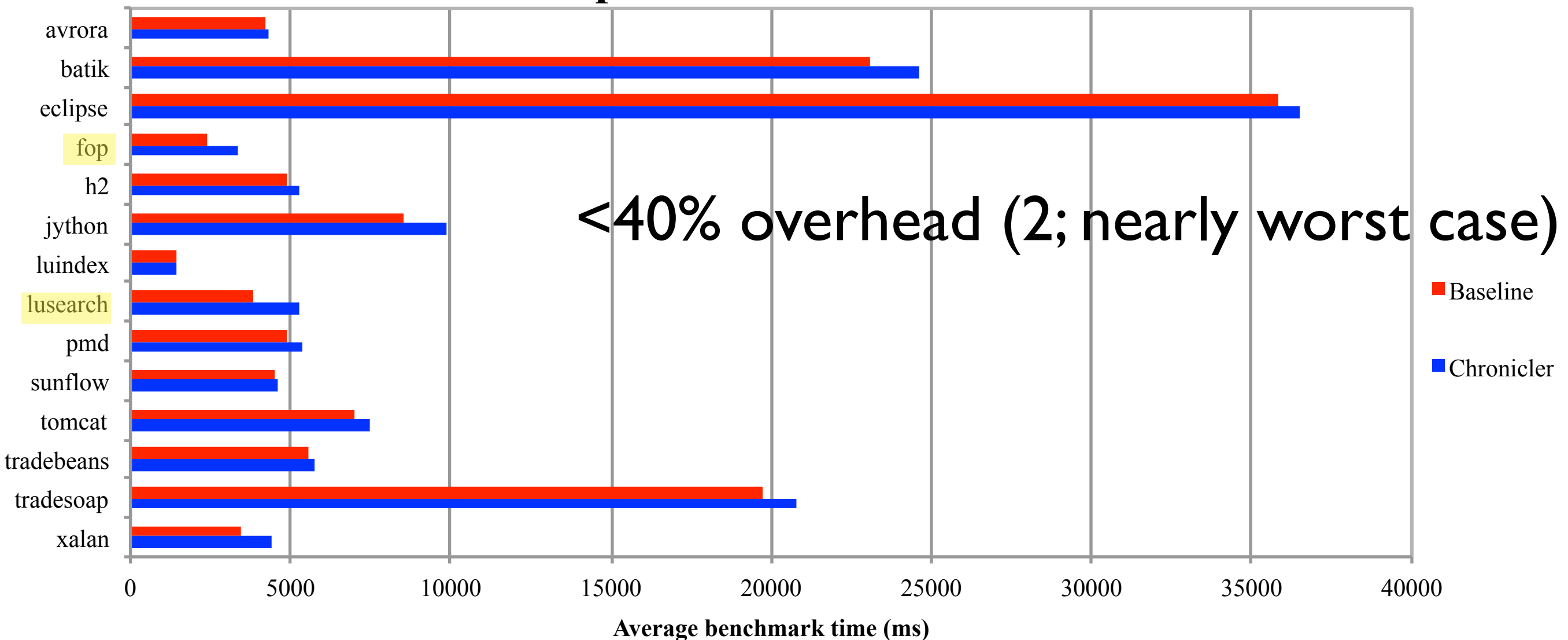
Performance: DaCapo

DaCapo Absolute Performance



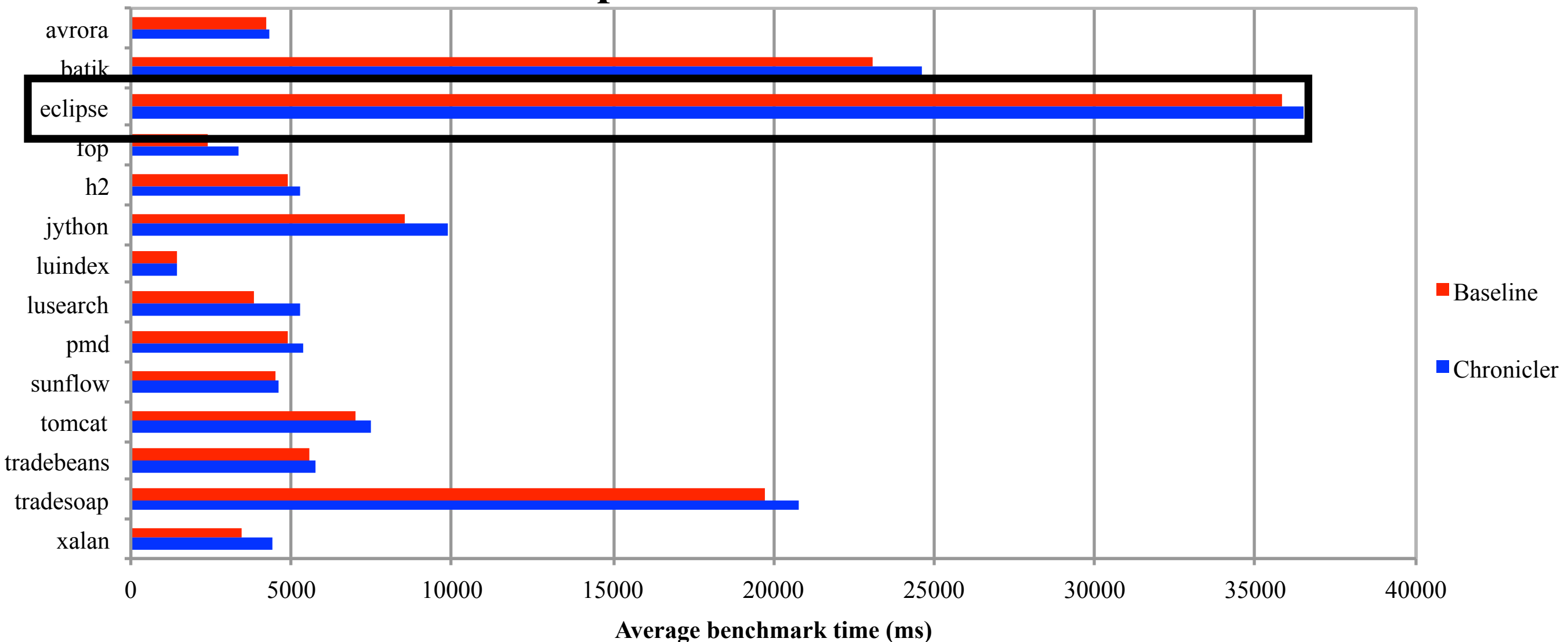
Performance: DaCapo

DaCapo Absolute Performance



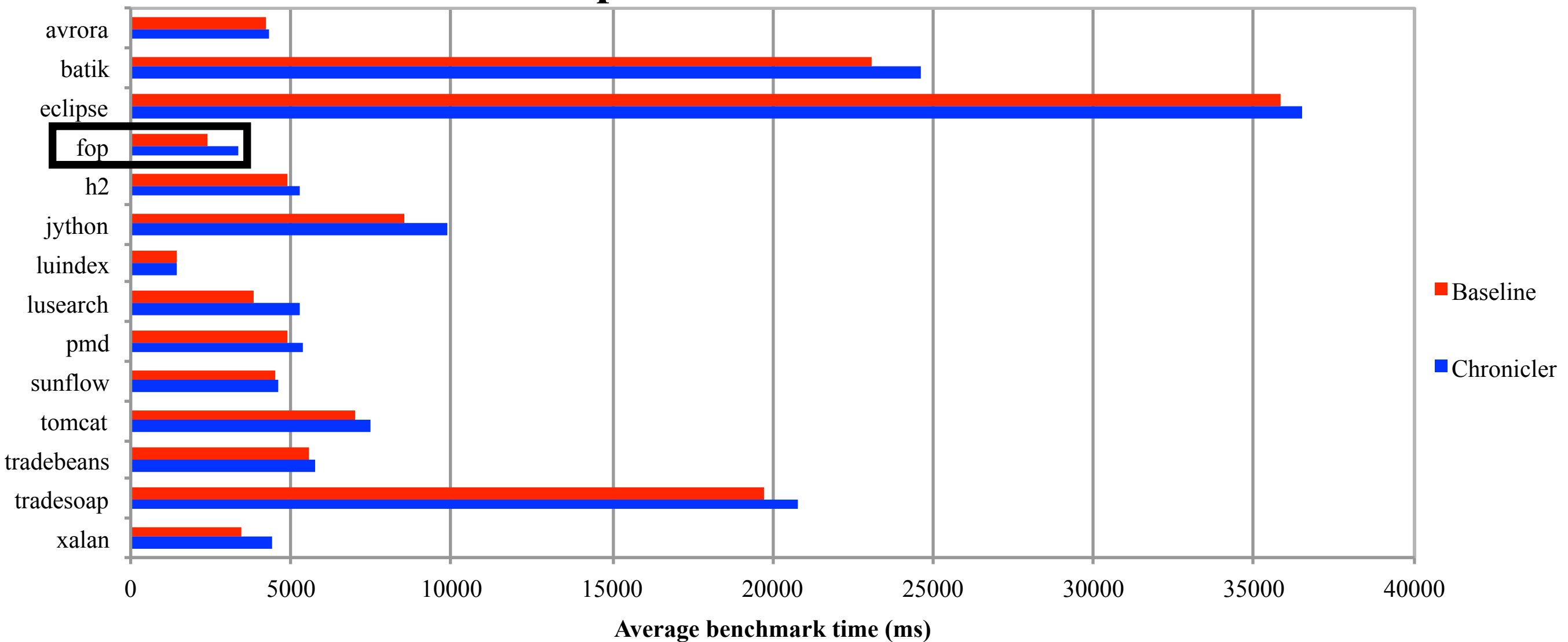
Performance: DaCapo

DaCapo Absolute Performance

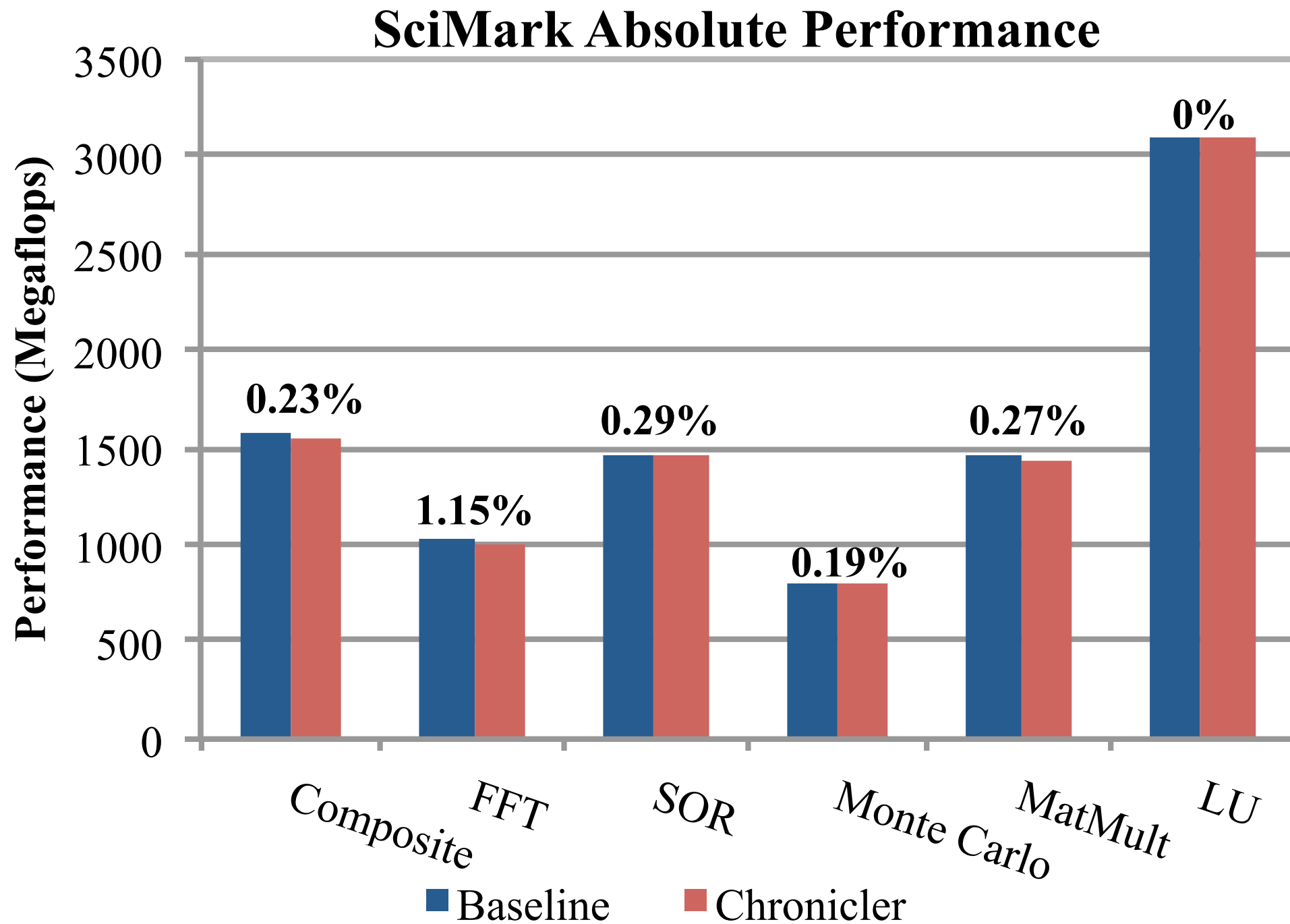


Performance: DaCapo

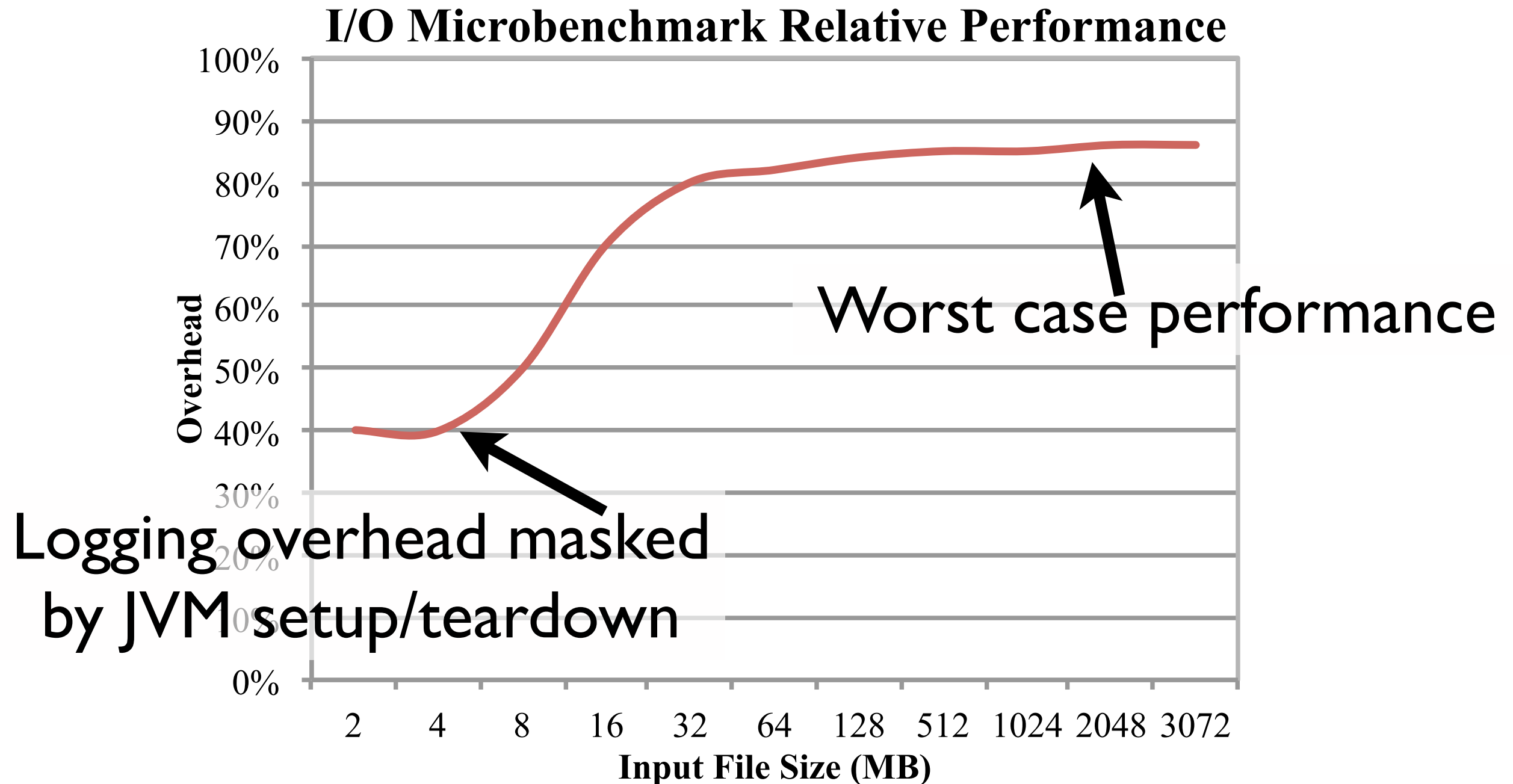
DaCapo Absolute Performance



Performance: Best Case



Performance: Worst Case



Limitations and Future Work

Limitations and Future Work

- Assumes VM correctness
- Thread Interleavings
 - Employ developer-side race detectors [e.g. Naik]
 - Integrate with existing thread access loggers [e.g. Huang]
- Privacy
 - Symbolic execution on the client to generate new inputs [e.g. Castro, Clause]

Chronicler: Lightweight Recording to Reproduce Field Failures

Jonathan Bell, Nikhil Sarda and Gail Kaiser
Columbia University, New York, NY USA

<https://github.com/Programming-Systems-Lab/chroniclerj>

jbell@cs.columbia.edu