DynamoRIO 介绍

刘阳 2023-09-23
南盘江计划

目录

DynamoRIO 介绍

- 简介和历史
- 介绍范围
- 用法
- 基本块和代码缓存
- 透明性
- 多架构支持

简介和历史

DynamoRIO 介绍

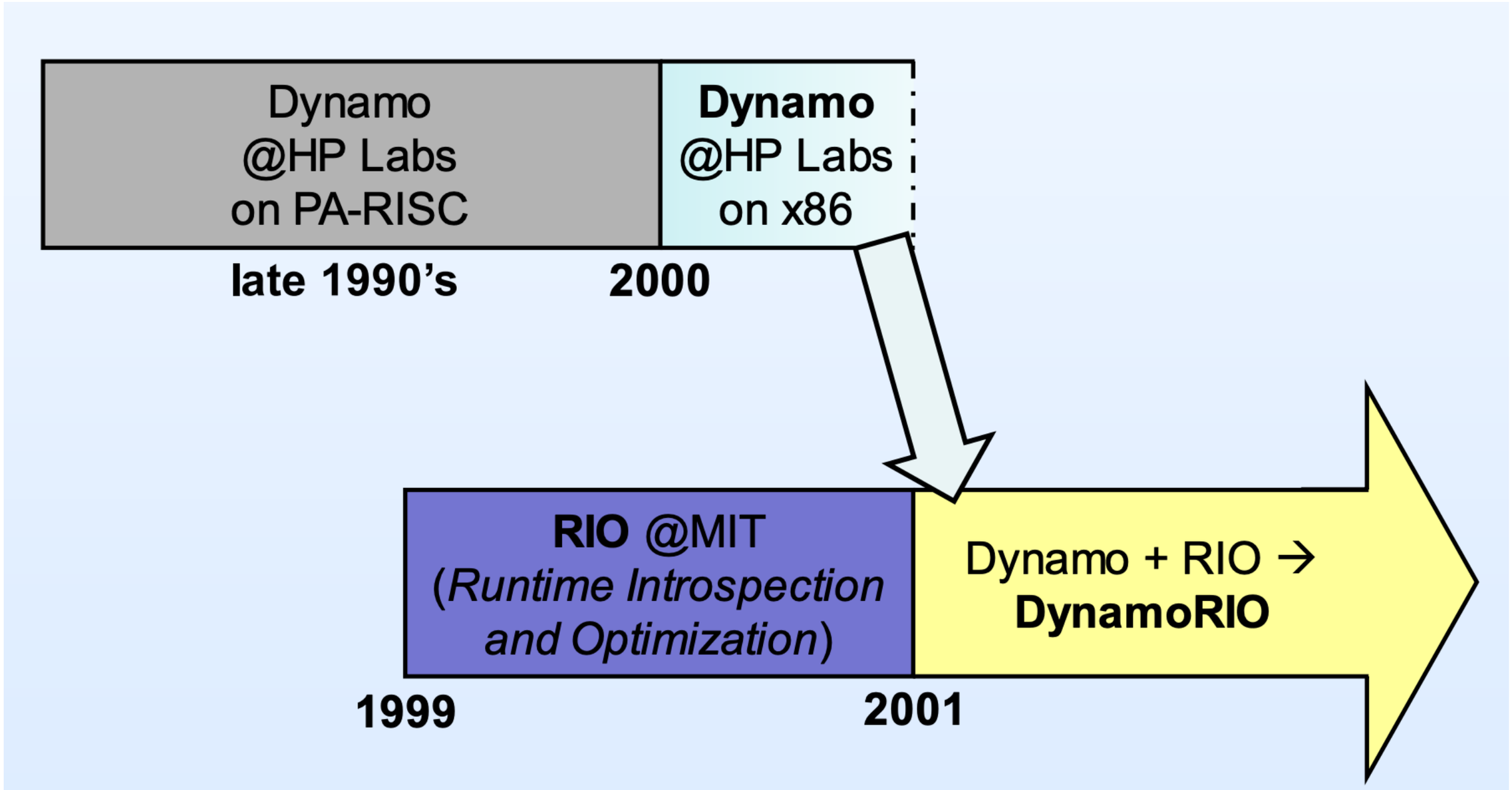
DynamoRIO is a runtime code manipulation system that supports code transformations on any part of a program, while it executes.

DynamoRIO 是一个运行时的代码修改系统，支持在程序运行时对其任意部分做代码转换。

https://dynamorio.org/

简介和历史

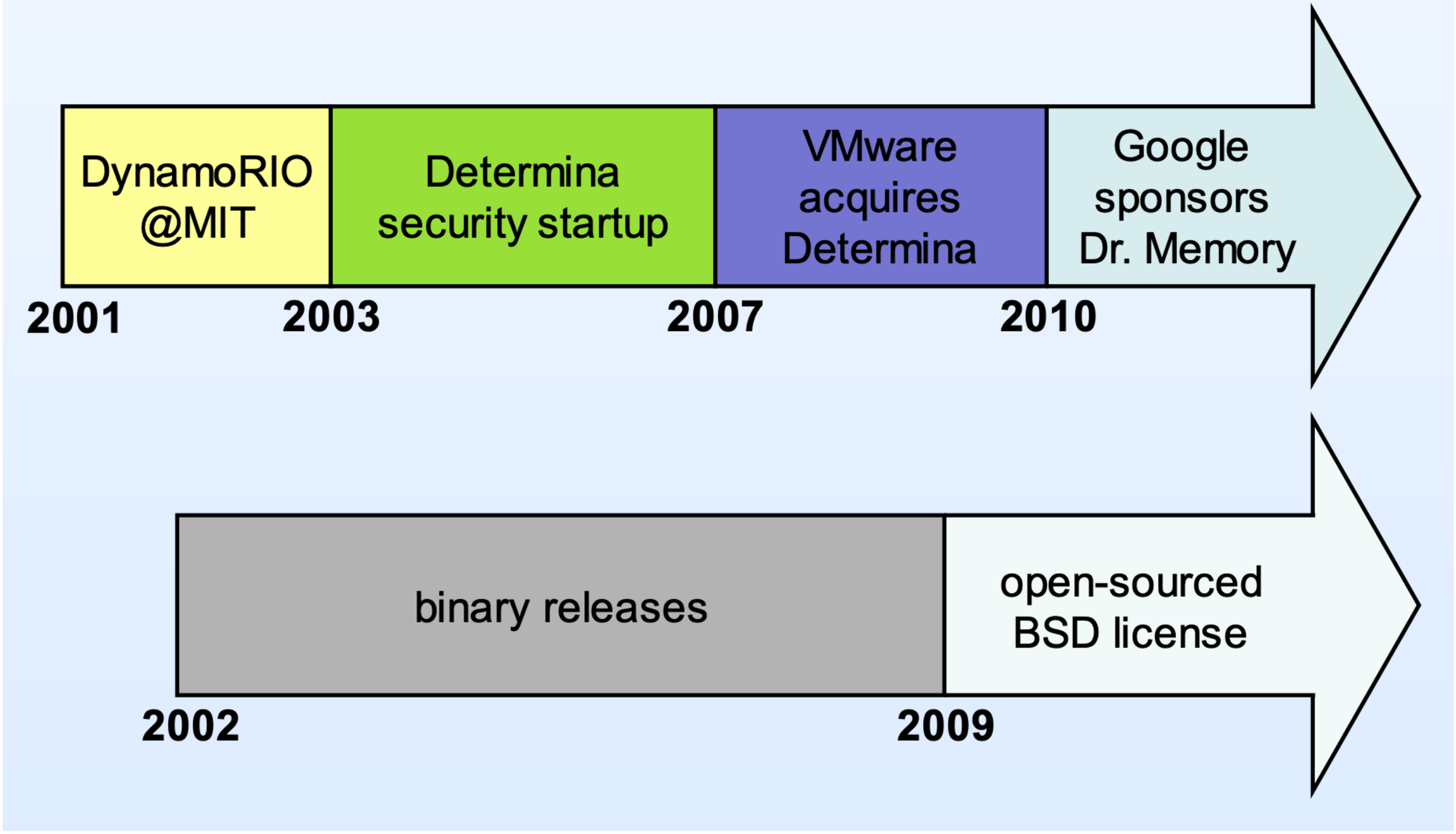
DynamoRIO 介绍



https://dynamorio.org/page_slides.html

简介和历史

DynamoRIO 介绍



https://dynamorio.org/page_slides.html

介绍范围

DynamoRIO 介绍

只介绍 DynamoRIO 本身

用法

DynamoRIO 介绍

```
drrun -t <client> -- <guest>
```

```
drrun -t drmemory -- chrome
```

用法

DynamoRIO 介绍

```
drrun -t <client> -- <guest>
```

Client 可以观察 guest 在运行过程中执行的**每一条指令**，对任意指令做出**任意修改**，可以在任意位置插入**任意指令**，除非 client 确实修改了 guest 的行为，否则 guest **无从知道自己正在被观察**。

性能损失极小：0～30%

可以运行在**常见硬件**上，且**不需要 root 权限**。

用法

DynamoRIO 介绍

```
drrun -t <client> -- <guest>
```

楚门的世界 + 盗梦空间

基本块和代码缓存

DynamoRIO 介绍

- Basic Block
- 以任意指令开头，以跳转指令结尾的指令序列，即每个基本块：
  - 由 >= 1 条指令组成
  - 有且只有一条跳转指令，且必须是最后一条指令

基本块和代码缓存

DynamoRIO 介绍

```
1   test:
2           li      a4,524288
3           add     a4,a0,a4
4   .L4:
5           fld     fa5,0(a1)
6           fld     fa4,0(a0)
7           addi    a1,a1,8
8           fgt.d   a5,fa5,fa4
9           beq     a5,zero,.L2
10          fsd     fa5,0(a0)
11  .L2:
12          addi    a0,a0,8
13          bne     a0,a4,.L4
14          ret
```

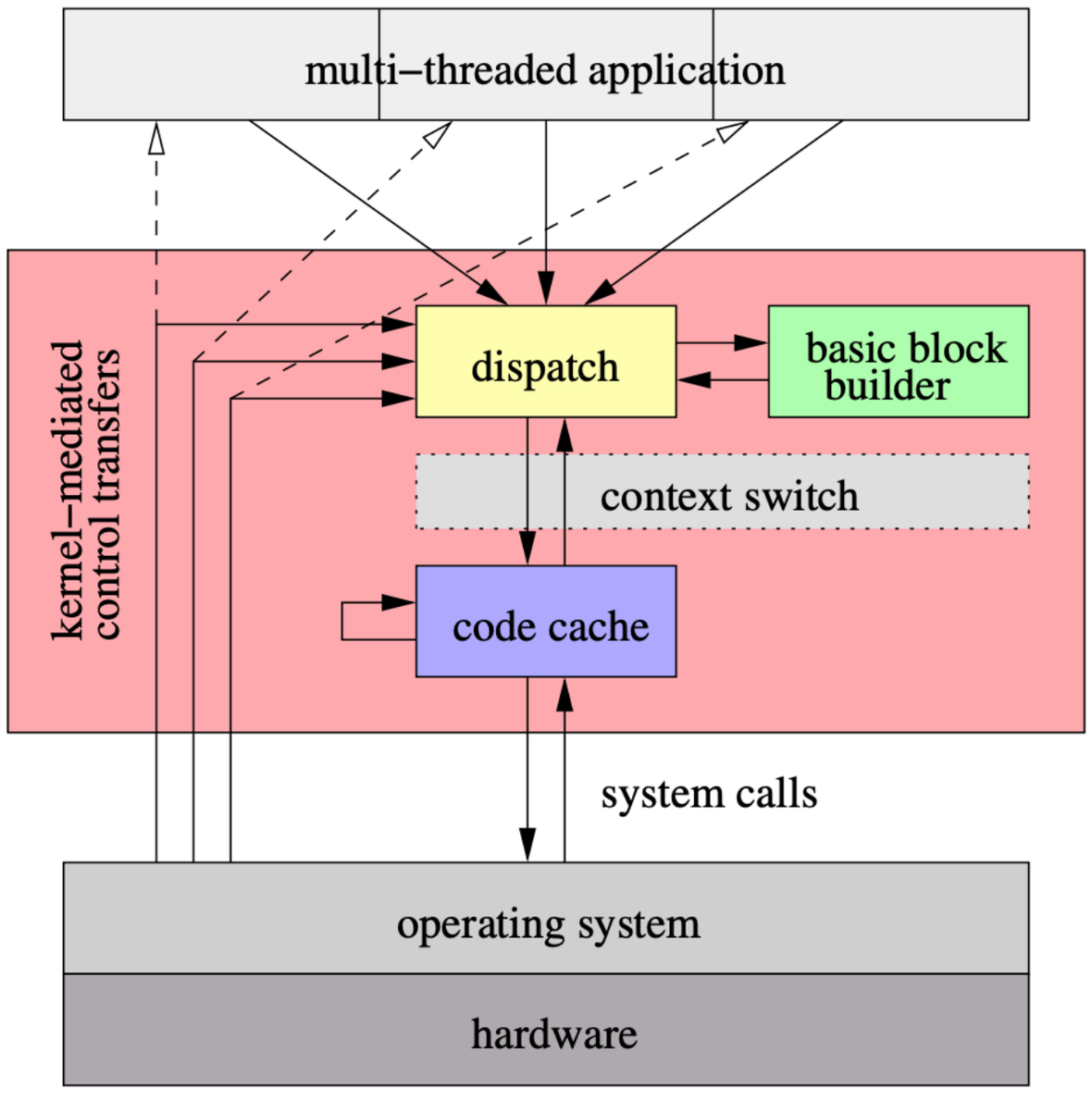
基本块和代码缓存

DynamoRIO 介绍

- DynamoRIO Basic Block
  - Runtime (JIT)
- LLVM IR Basic Block：
  - Ahead of Time

基本块和代码缓存

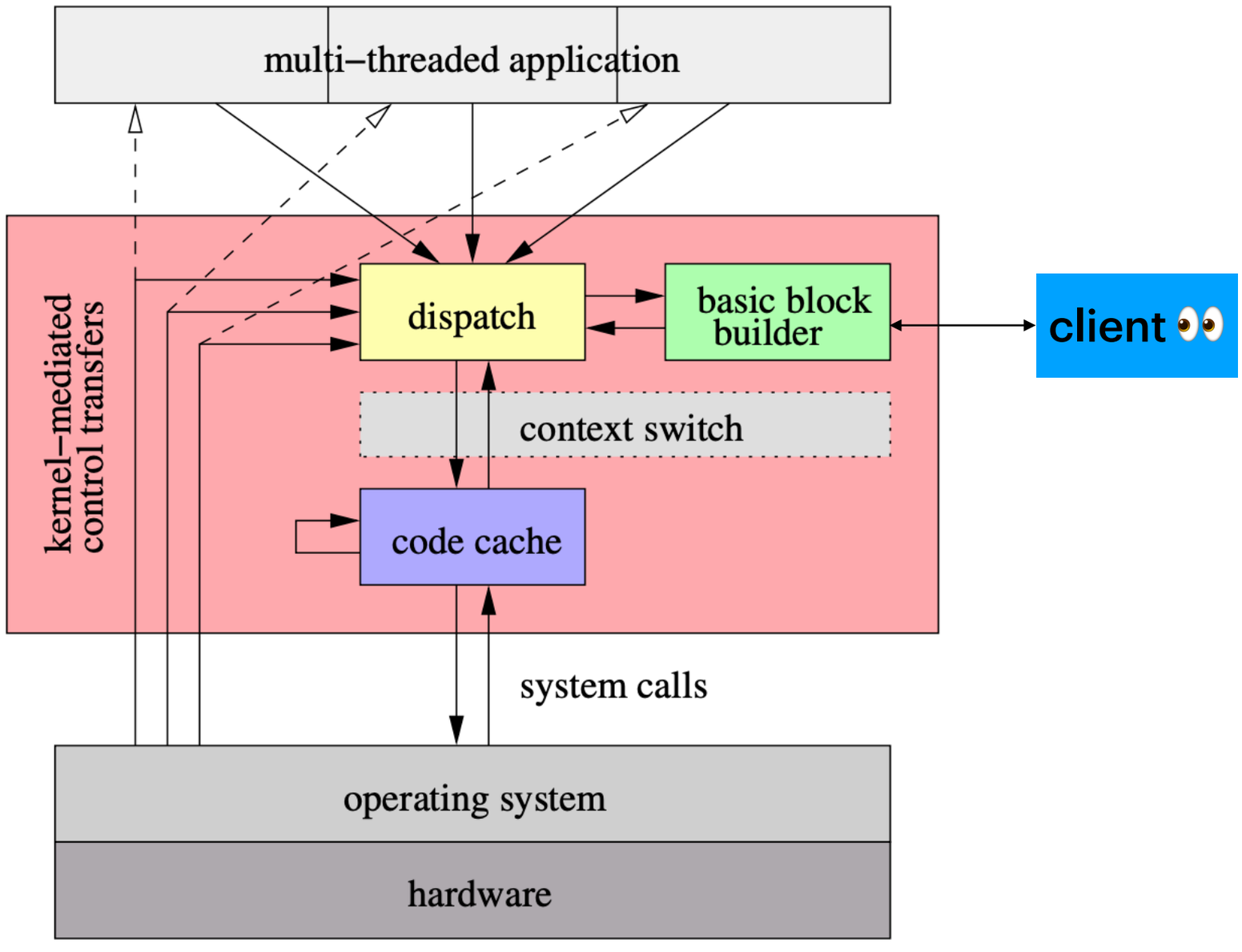
DynamoRIO 介绍



https://dynamorio.org/

基本块和代码缓存

DynamoRIO 介绍



https://dynamorio.org/

基本块和代码缓存

DynamoRIO 介绍

Client 可以观察 guest 在运行过程中执行的**每一条指令**，对任意指令做出**任意修改**，可以在任意位置插入**任意指令**，除非 client 确实修改了 guest 的行为，否则 guest **无从知道自己正在被观察。**

性能损失极小：0～30%

可以运行在**常见硬件**上，且**不需要 root 权限。**

透明性

DynamoRIO 介绍

DynamoRIO 必须**完全透明**。

透明性

DynamoRIO 介绍

挑战：

- 在任何时候都保持控制权
- code cache
- 不能对程序的执行做任何假设
- 资源冲突（e.g. 不可重入）
- 多线程
- ....

透明性

DynamoRIO 介绍

方式：

- 不依赖外部库
- 位置无关代码 -> 位置相关代码

多架构支持

DynamoRIO 介绍

- x86
- x86-64
- ARM
- AArch64
- RISCV64 -- ongoing 20%

- Windows
- Linux
- macOS

链接

DynamoRIO 介绍

- https://dynamorio.org/
- https://github.com/DynamoRIO/dynamorio

谢谢

Q & A