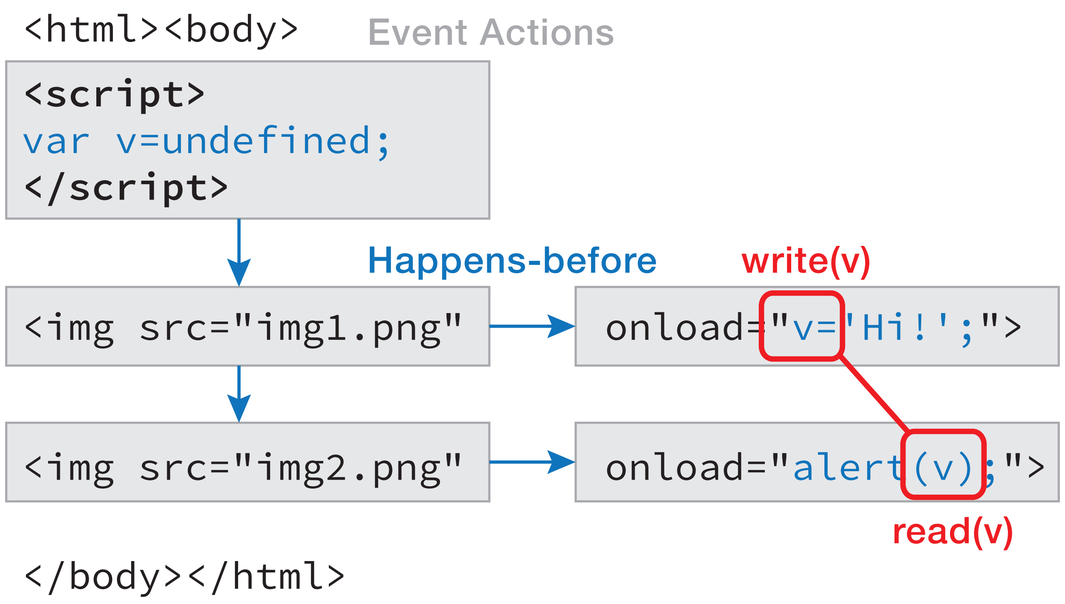
EVENT RACER

www.eventracer.org, www.github.com/eth-srl

Finding Bugs in Event-Driven Applications

Pavol Bielik, ETH Zurich

Web Page Concurrency



Android Concurrency

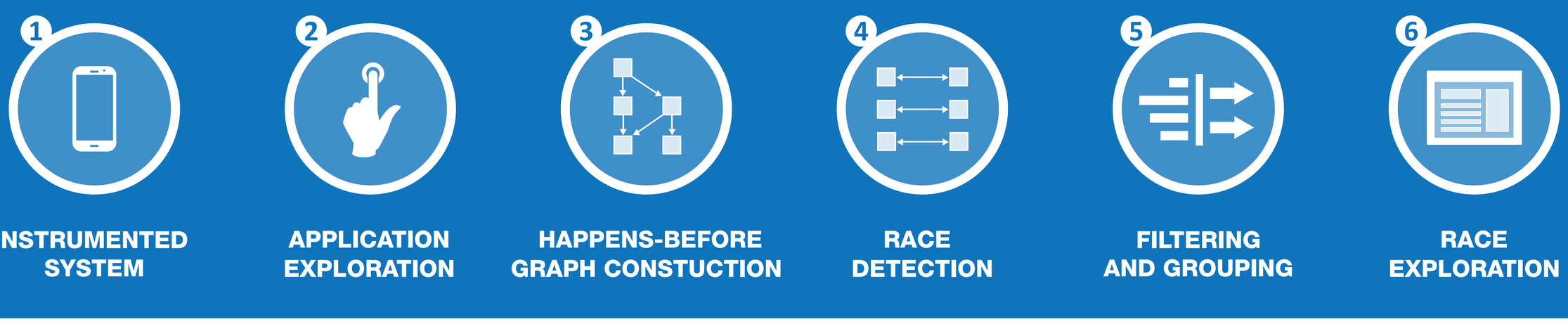
```
protected void onCreate() {
  requestLocationUpdates(GPS, 0, 0, mListener);
  mDbHelper = new SQLiteOpenHelper(this, DB_NAME, DB_VERSION);
}
```

↓

```
LocationListener mListener = new LocationListener() {
  public void onLocationChanged(Location location) {
    //show location on map
    mDbHelper.insert(loc);
  }
};
```

↓ ?

```
protected void onStop() {
  removeUpdates(mListener);
  mDbHelper.close();
}
```



Instrumented System

What are the memory locations on which operations can race?

JS VARIABLES, FUNCTIONS, ARRAYS

```
v='Hi!';                    →  write(v)
function f() {}             →  write(f)
messages[2] = 42;           →  write(messages[2])
```

DOM NODES, ATTRIBUTES

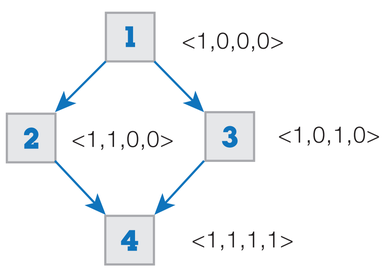
```
<img id="img1" src="img1.png"
     onload="v='Hi!';">     →  write(#img1)
                               write(#img1.onload)

document.getElementById("img1")
     .addEventListener("click", f);  →  read(#img1)
                                        write(#img1.click)
```

Race Detection

How to make scalable race detection in event-based setting?

VECTOR CLOCKS

O(1) >0.1s O(N*N) 544MB



VECTOR CLOCKS + CHAINED DECOMPOSITION

O(1) 0.04s O(N*C) 5MB

$2 \leq 4$

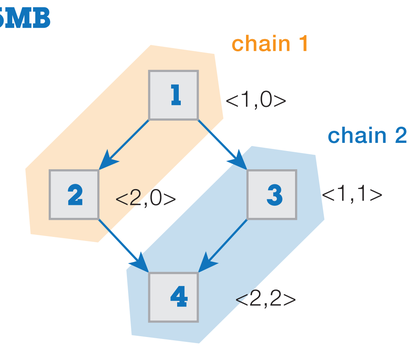
$\langle 1,1,0,0\rangle \leq \langle 1,1,1,1\rangle$

$\langle 2,0\rangle \leq \langle 2,2\rangle$

$2 \not\leq 3$

$\langle 1,1,0,0\rangle \not\leq \langle 1,0,1,0\rangle$

$\langle 2,0\rangle \not\leq \langle 1,1\rangle$



Happens-before Graph Construction

What is the event happens-before?

DOCUMENTATION

public void removeUpdates (LocationListener listener)

Added in API level 1

Remove all location updates for the specified LocationListener. Following this call, updates will no longer occur for this listener.

FORMALIZE API HAPPENS-BEFORE

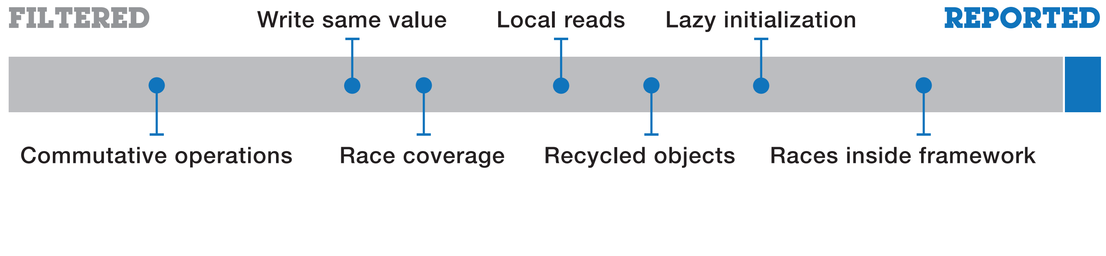
setInterval, SetTimeout, AJAX, ...

postDelayed, postAtFront, postIdle, IPC, Handler, Threads, ThreadPools, ...

Race Filtering and Grouping

How to produce feasible amount of reports?

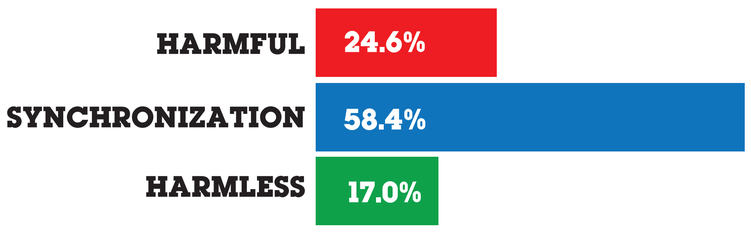
1328 646 → 17.8 13



Evaluation

Is the system effective at finding harmful races?

Fortune 100 Web Pages (314 reports)

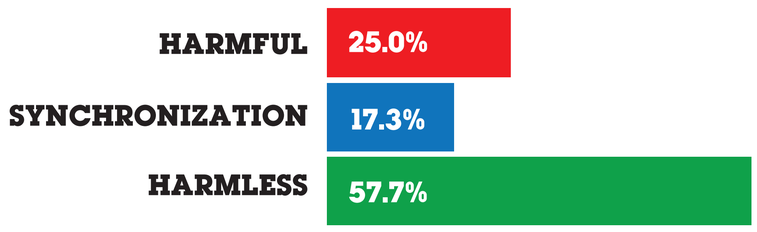


Non-operational menu

Non-deterministic jQuery version

Incomplete form submitted

8 Google Play Store Applications (104 reports)



NPR News — Display same article twice

OI File Manager — Display wrong directory

Flickr Uploader — Display images in wrong order

Veselin Raychev, Pavol Bielik, Martin Vechev

ETH zürich

Manu Sridharan

SAMSUNG RESEARCH AMERICA