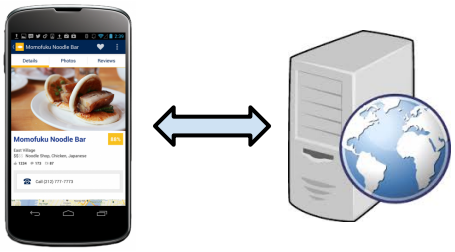
A Large Scale Security Analysis of Mobile Web Apps

Patrick Mutchler, Adam Doupé, John Mitchell, Chris Kruegel, and Giovanni Vigna

What is a Mobile Web App?

Mobile Web Apps use embedded web browsers to manage user interaction.



The JavaScript Bridge

Apps can expose Java objects to JS code running in embedded browser. JS code from any origin has access to them!

```
// Java code
addJavascriptInterface(obj, 'o');

// JavaScript code
o.foo(); // calls obj's method foo
```

A Serious Exploit

```
// Uses a Bridge Object to run a shell
o.getClass().forName('java.lang.Runtime').
   getMethod('getRuntime', null).
   invoke(null, null).exec('/system/bin/sh');
```

Remote Code Execution!

- Delete or steal files
- Install malware
- Send premium SMS
- Crash the phone
- etc...

Who is Vulnerable?

Apps that use the JS Bridge and run untrusted scripts are vulnerable. Common ways of running untrusted scripts are:

- Using HTTP
- Using HTTPS incorrectly
- Navigating to untrusted pages

Experimental Results

737,828 apps from Google Play
563,109 mobile web apps
219,404 use the JS Bridge
13,683 navigate to untrusted pages
36,292 use HTTP
18,794 use HTTPS incorrectly
45,689 unique vulnerable apps