A WEBSITE IN YOUR POCKET:
A LARGE-SCALE SECURITY ANALYSIS OF MOBILE WEB APPS

Patrick Mutchler
Adam Doupe (UCSB)

John Mitchell
Chris Kruegel (UCSB)
Giovanni Vigna (UCSB)
What is a Mobile Web App?
Unique Features of Mobile Web Apps
Navigation Control
public boolean shouldOverrideUrlLoading(WebView view, String url) {

    // False -> Load url in WebView
    // True   -> Load url in default browser

}
public boolean shouldOverrideUrlLoading(WebView view, String url) {

    String host = new URL(url).getHost();
    if (host.equals("stanford.edu"))
        return false;
    return true;
}

JavaScript Bridge
addJavascriptInterface(foo, 'f');
f.bar();
Q: Who has access to the bridge?
Q: Who has access to the bridge?

A: Everybody
Q: Who has access to the bridge?

A: Everybody

No longer safe to frame untrusted content!
Q: How bad is this?
Q: How bad is this?
A: Very bad
Q: How bad is this?

A: Very bad

// foo is a Bridge Reference
foo.getClass().forName("java.lang.Runtime").
    getMethod("getRuntime", null).
    invoke(null, null).exec("/system/bin/sh");
for(prop in window){
    obj = window[prop];
    if(obj !== null && typeof(obj) === "object"){
        num_prop = 0;
        for(prop in obj)
            num_prop += 1

        if(num_prop == 0 && "hashCode" in obj)
            return obj;
    }
}
for(prop in window){
  obj = window[prop];
  if(obj !== null && typeof(obj) === "object"){
    num_prop = 0;
    for(prop in obj) num_prop += 1;
    if(num_prop === 0 && "hashCode" in obj) return obj;
  }
}
• @JavascriptInterface
  • Android 4.2 (Nov, 2012)
• @JavascriptInterface
  • Android 4.2 (Nov, 2012)

• 73% of devices in use (Feb, 2014)
• 82% of free apps (Oct, 2013)
• 64% of updated free apps updated (Oct, 2013)
• @JavascriptInterface
  • Android 4.2 (Nov, 2012)

• 73% of devices in use (Feb, 2014)
• 82% of free apps (Oct, 2013)
• 64% of updated free apps updated (Oct, 2013)

• Both device and app must be safe
Untrusted content must never be rendered

1. Prevent navigation to untrusted URLs
2. Do not frame untrusted content
3. Use HTTPS correctly
4. …
Experimental Results
• 737,828 free apps from Google Play (Oct ’13)
• 563,109 apps use a WebView
• 545,415 enable JavaScript
• 524,582 implement shouldOverrideUrlLoading
• 219,404 use the JavaScript Bridge
40,084 apps with full URLs and Bridge Objects
13,683 apps (34%) reach untrusted content
152,706 apps with partially computed URLs
87,968 apps (57%) with HTTP URLs

- 59% No Bridge Object
- 34% Vulnerable on all devices
- 7% Vulnerable on some devices
onReceivedSslError

1. handler.proceed()
2. handler.cancel()
3. view.loadUrl(...)

public void onReceivedSslError(
    WebView view,
    SslErrorHandler handler,
    SslError error){

    handler.proceed();
}

117,974 apps implement `onReceivedSslError`
29,652 apps (25%) must ignore errors
# apps vulnerable on safe devices?

37,418
# apps vulnerable on unsafe devices?

45,689
Other Fun

- HTML from shared filesystem
Other Fun

- HTML from shared filesystem
- CSRF like attack
Other Fun

• HTML from shared filesystem

• CSRF like attack

• Expired domain name attack
Other Fun

- HTML from shared filesystem
- CSRF like attack
- Expired domain name attack
- Silk Browser (Kindle Fire)
Other Fun

- HTML from shared filesystem
- CSRF like attack
- Expired domain name attack
- Silk Browser (Kindle Fire)
- searchBoxJavaBridge_
Questions?