COMPUTER SCIENCE
& ENGINEERING
TEXAS A&M UNIVERSITY

Iframes/Popups Are Dangerous in Mobile WebView: Studying and Mitigating Differential Context Vulnerabilities

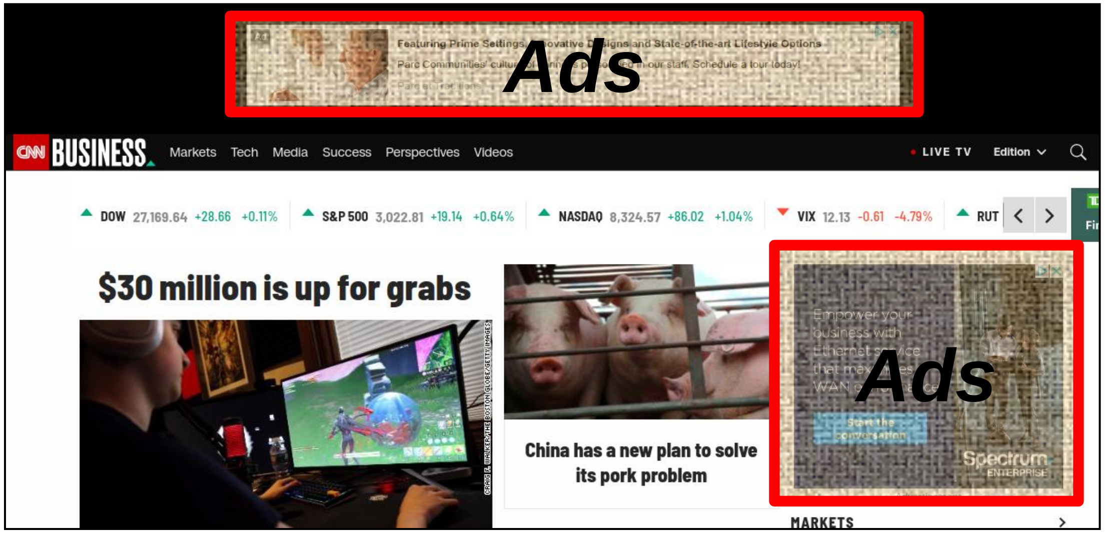
***Guangliang Yang**, Jeff Huang, and Guofei Gu*

*__S__ec**u**re **C**ommunication and **C**omput**e**r **S**y**s**tems Lab

Texas A&M University

Iframes/Popups in Regular Browsers

- In modern web apps, iframes/popups are frequently used. Their security has been well studied in regular browsers.


Ads
CNN BUSINESS
Markets
Tech
Media
Success
Perspectives
Videos
LIVE TV
Edition
DOW 27,169.64 +28.66 +0.11%
S&P 500 3,022.81 +19.14 +0.64%
NASDAQ 8,324.57 +86.02 +1.04%
VIX 12.13 -0.61 -4.79%
RUT
$30 million is up for grabs
China has a new plan to solve its pork problem
Ads
Spectrum ENTERPRISE
MARKETS

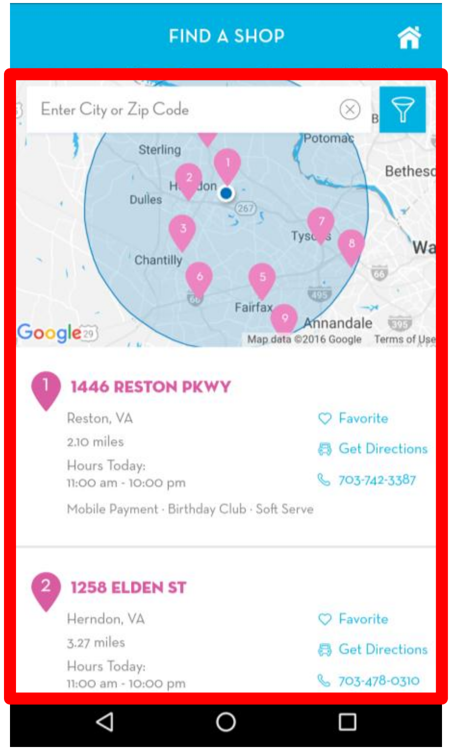
Iframes/Popups in Regular Browsers

- In modern web apps, iframes/popups are frequently used. Their security has been well studied in regular browsers.

- However, the security study on a *new web environment*, called mobile **WebView**, is still missing.

WebView

- An embedded browser-like UI component in mobile apps (i.e., hybrid apps)
- Easy to use and powerful
- Frequently used by mobile apps
  - Integrated in ~80% Android apps



FIND A SHOP

Enter City or Zip Code

1446 RESTON PKWY
Reston, VA
2.10 miles
Hours Today:
11:00 am - 10:00 pm
Favorite
Get Directions
703-742-3387
Mobile Payment · Birthday Club · Soft Serve

1258 ELDEN ST
Herndon, VA
3.27 miles
Hours Today:
11:00 am - 10:00 pm
Favorite
Get Directions
703-478-0310

Motivation & Our Work

- WebView provides a totally new working environment for iframes/popups.

=> ***Are iframes/popups still safe in WebView?***

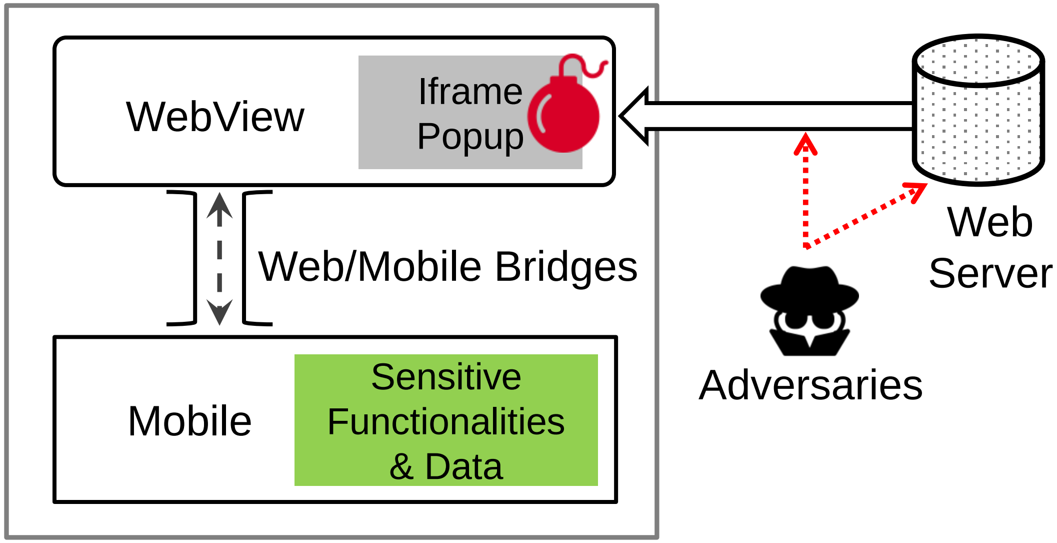
Motivation & Our Work

- We conduct the first security study in Android WebView => ***Differential Context Vulnerabilities*** (DCVs)
- We assess the security impacts on real-world apps with DCV-Hunter:
  - Facebook, Instagram, Facebook Messenger, Google News, Skype, Uber, Yelp, and U.S. Bank …
- We propose a novel multi-layer defense solution.

Security Study & DCV

Threat Model

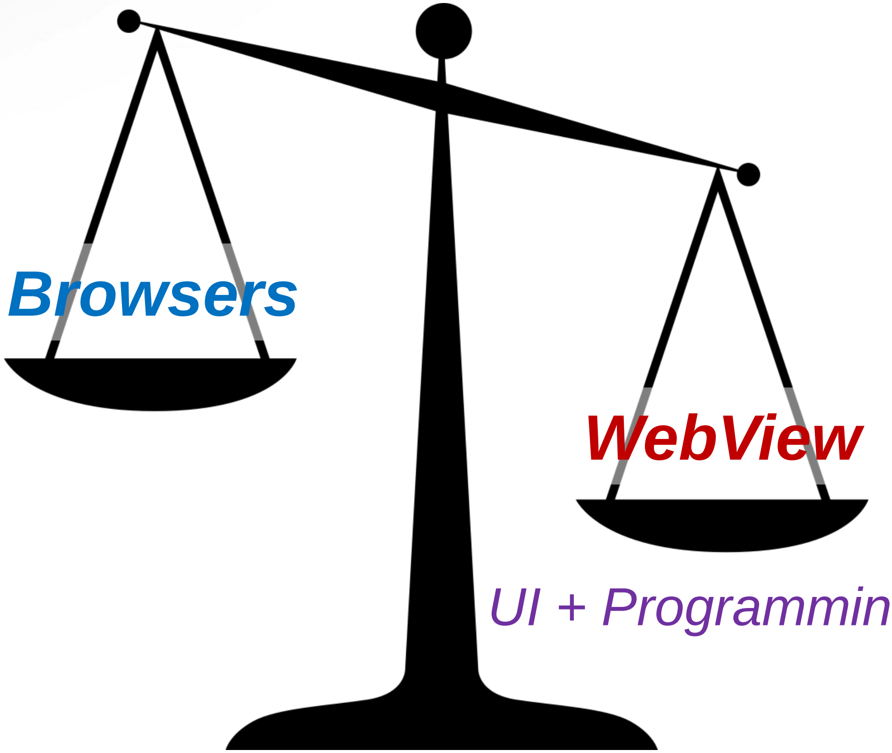
- Mobile code is benign
- WebView may contain untrusted content
  - The main (top) frame is trusted
  - Iframes/popups loading third-party content are ***untrusted***.



Benign Hybrid App

Security Study

Inconsistencies Between Browsers and WebView

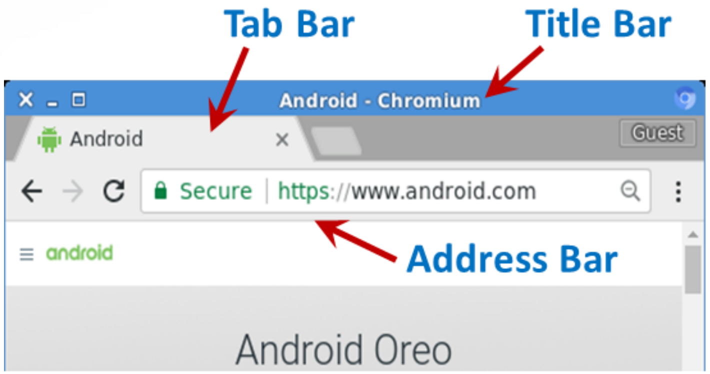


UI + Programming Features

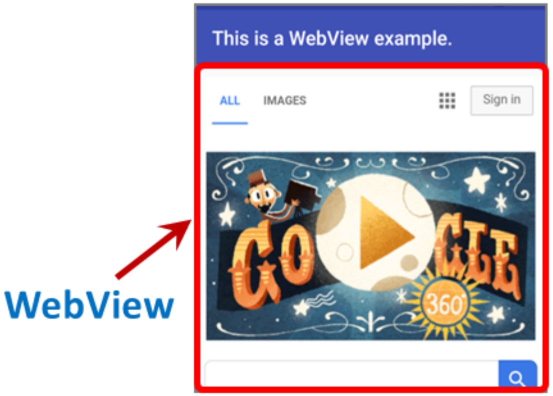
Possible Attacks: *Untrusted iframes/popups may trigger and leverage these inconsistencies to obtain risky abilities.*

Inconsistencies Between Browsers and WebView

- UI Design Styles



(a) Regular Browser UI



(b) WebView UI

Security Issues & Concrete Attacks

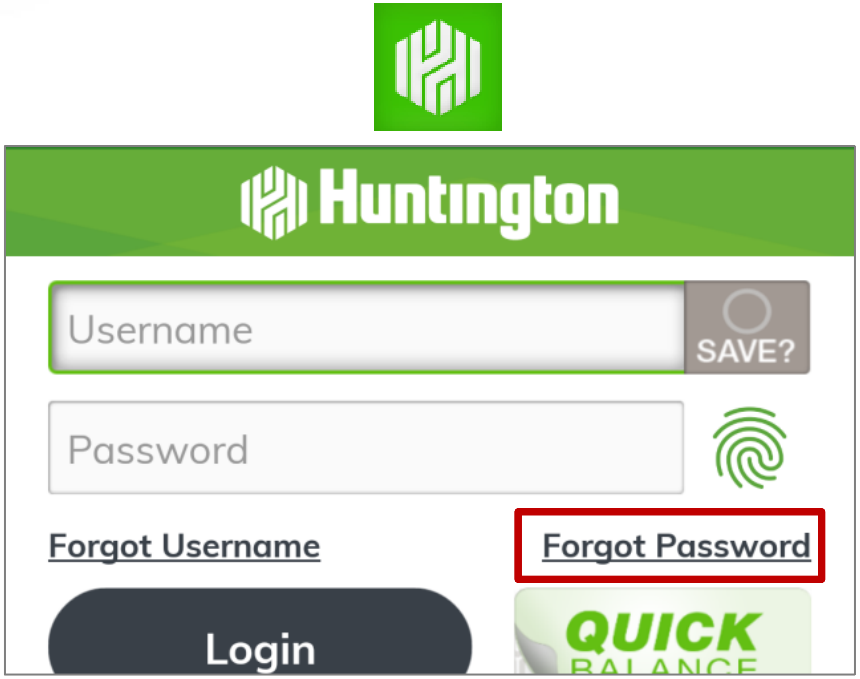
- The lack of the address bar

  => ***Main-Frame Navigation Attacks***: *Untrusted iframes/popups launch phishing attacks by secretly navigating the main frame.*

- Permissive navigation policy
  - Any sub-frame can navigate the main frame
  - Not harmful in regular browsers
    - iframe sandbox + address bar
  - But dangerous in WebView

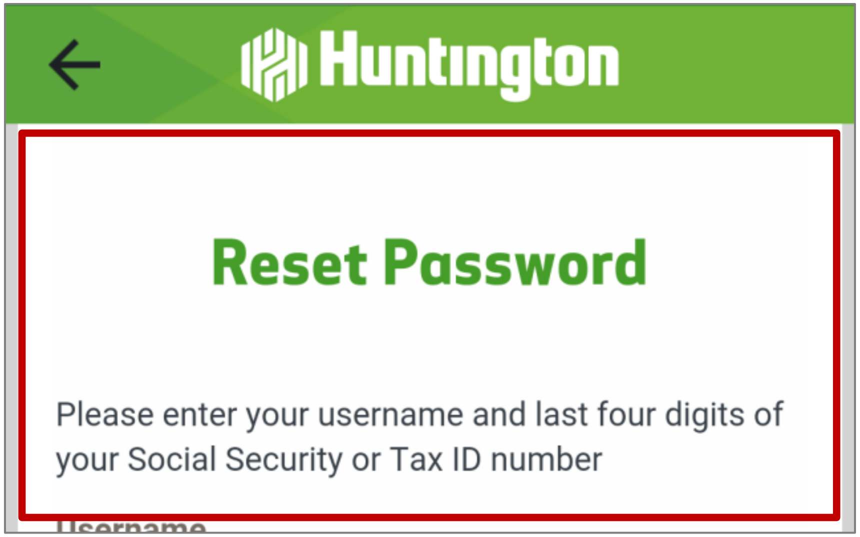
Security Issues & Concrete Attacks

- Example: A banking app



Security Issues & Concrete Attacks

- Example: A banking app



Huntington

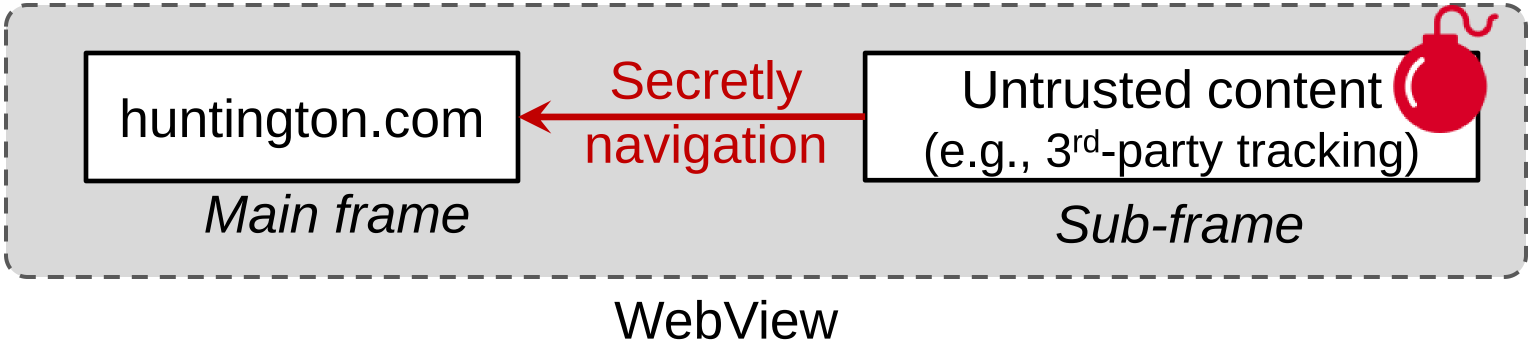
Reset Password

Please enter your username and last four digits of your Social Security or Tax ID number

Username

Security Issues & Concrete Attacks

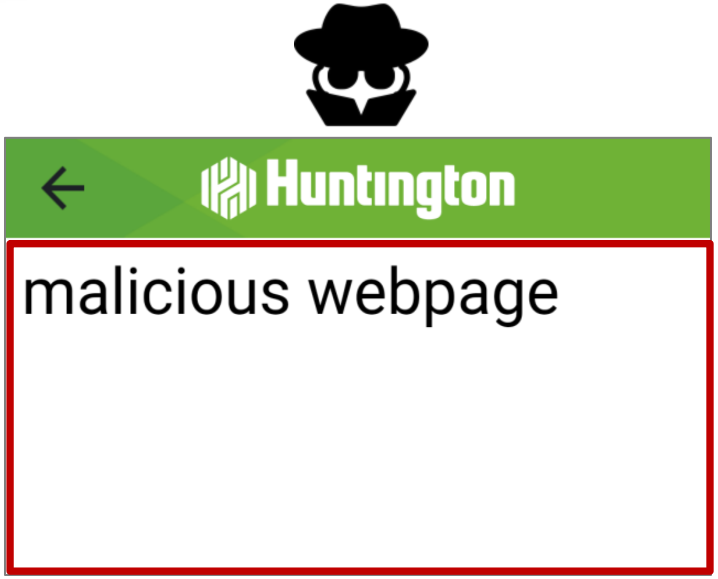
- Example: A banking app



window.open("http://attacker.com", "_top")

Security Issues & Concrete Attacks

- Example: A banking app



malicious webpage

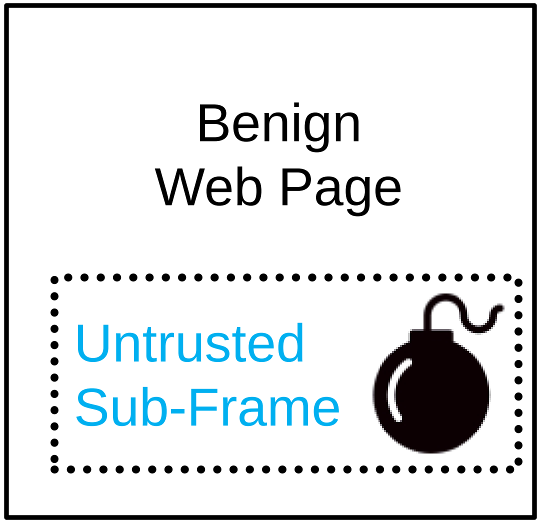
Security Issues & Concrete Attacks

- The lack of the tab bar
- Principles
  - Each web window is rendered by an independent WebView UI

=> ***WebView UI (WUI) Redressing Attacks***: *Untrusted iframes/popups launch phishing attacks by creating a malicious WUI and overlapping begin WUI with the new WUI.*

Security Issues & Concrete Attacks

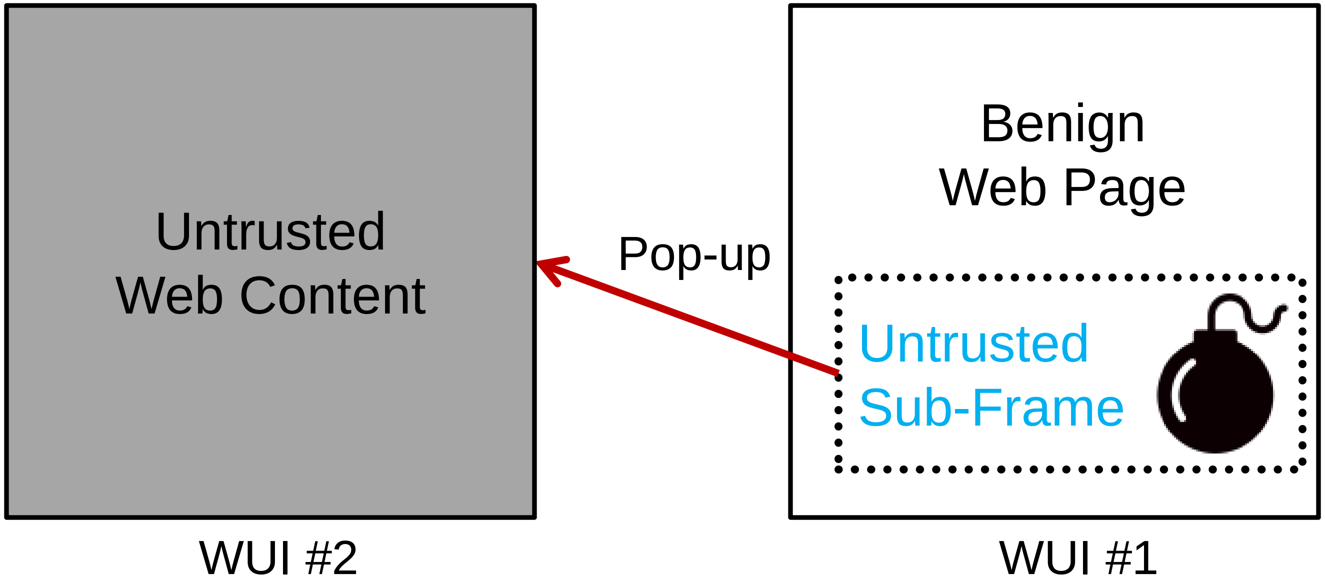
- WUI Redressing Attacks



WUI #1

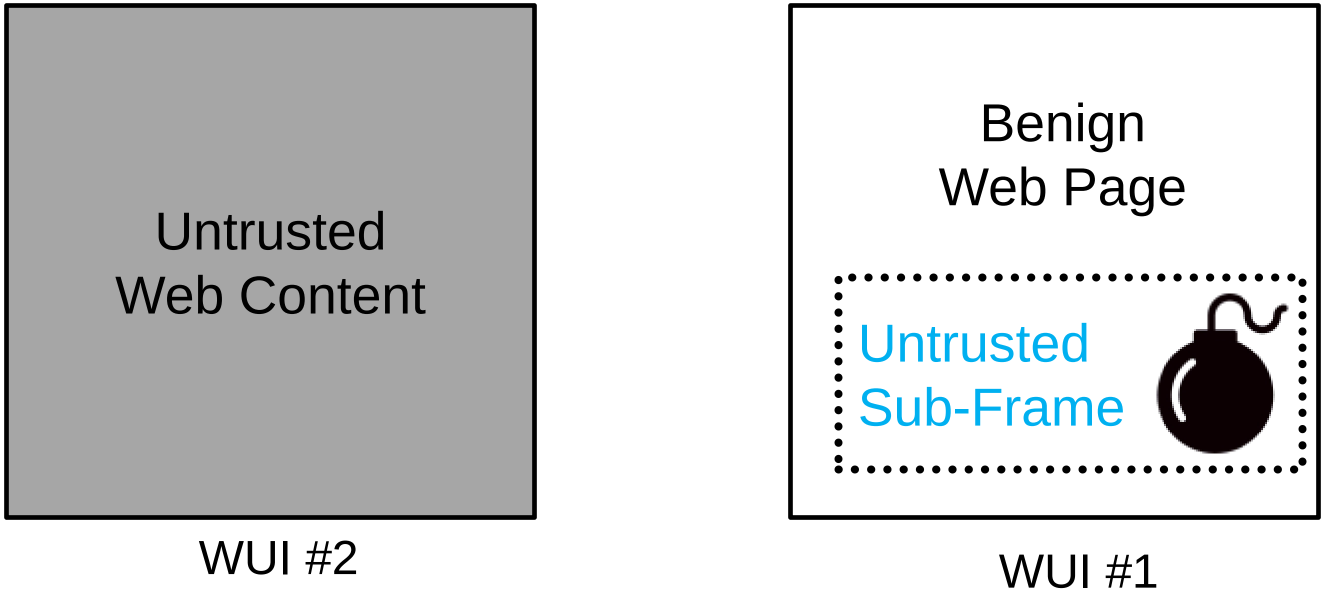
Security Issues & Concrete Attacks

- WUI Redressing Attacks
  - Possible Attack #1: Overlap attack
    - Manipulating the rendering order of multiple WUIs



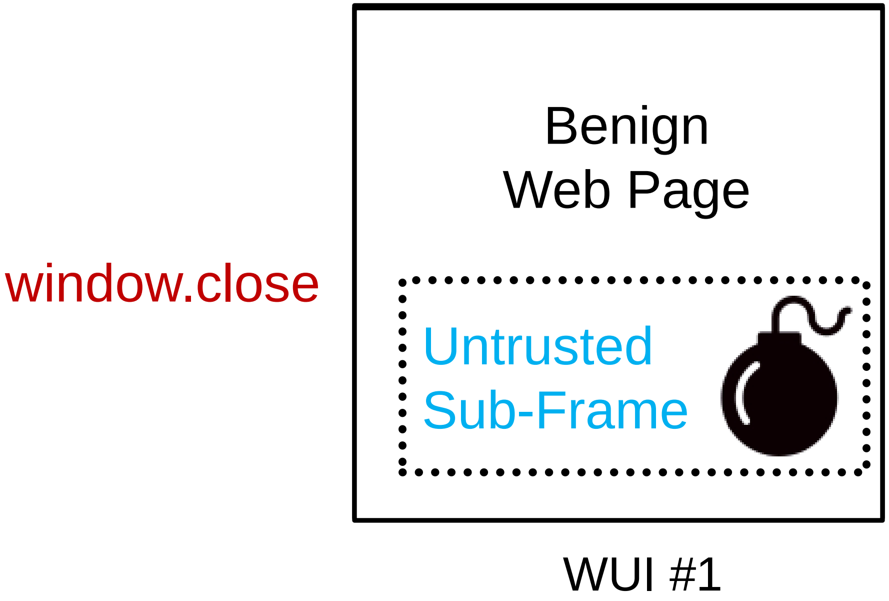
Security Issues & Concrete Attacks

- WUI Redressing Attacks
  - Possible Attack #2: Closure attack



Security Issues & Concrete Attacks

- WUI Redressing Attacks
  - Possible Attack #2: Closure attack



window.close

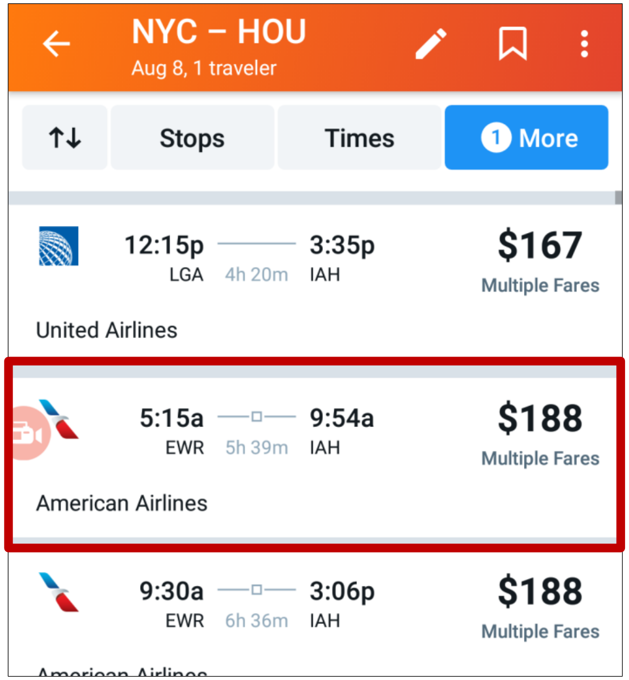
Benign Web Page

Untrusted Sub-Frame

WUI #1

Security Issues & Concrete Attacks

- Example: a flight searching app



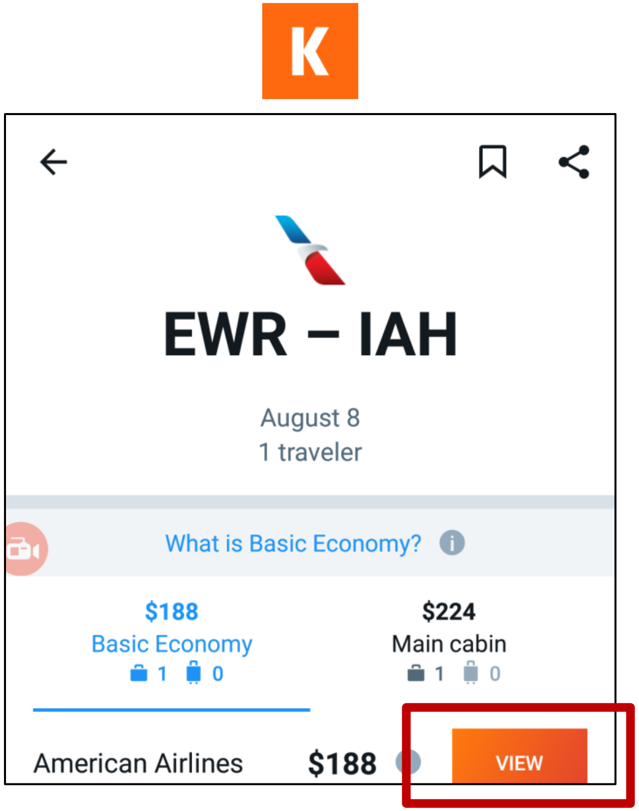
12:15p LGA — 4h 20m — 3:35p IAH $167 Multiple Fares
United Airlines

5:15a EWR — 5h 39m — 9:54a IAH $188 Multiple Fares
American Airlines

9:30a EWR — 6h 36m — 3:06p IAH $188 Multiple Fares
American Airlines

Security Issues & Concrete Attacks

- Example: a flight searching app



EWR – IAH

August 8
1 traveler

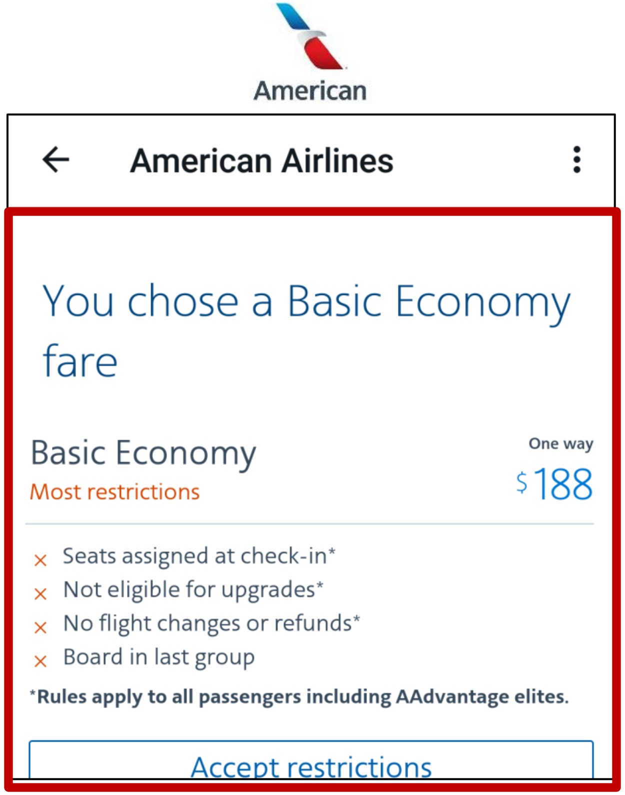
What is Basic Economy?

$188 Basic Economy 1 0	$224 Main cabin 1 0

American Airlines $188 VIEW

Security Issues & Concrete Attacks

- Example: a flight searching app



You chose a Basic Economy fare

Basic Economy
Most restrictions

One way
$188

× Seats assigned at check-in*
× Not eligible for upgrades*
× No flight changes or refunds*
× Board in last group

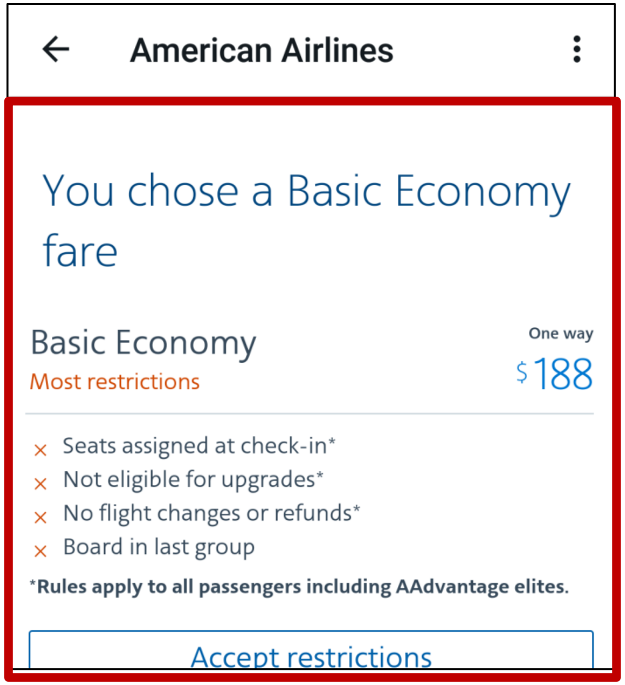
*Rules apply to all passengers including AAdvantage elites.

Security Issues & Concrete Attacks

- Example: a flight searching app

malicious webpage

American



← American Airlines ⋮

You chose a Basic Economy fare

Basic Economy
Most restrictions

One way
$188

× Seats assigned at check-in*
× Not eligible for upgrades*
× No flight changes or refunds*
× Board in last group

*Rules apply to all passengers including AAdvantage elites.

Inconsistencies Between Browsers and WebView

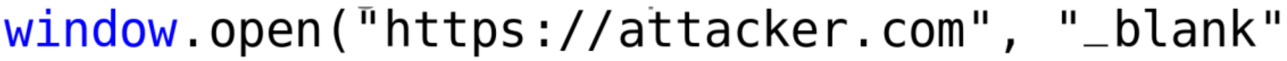
- Programming features
  - WebView enables many programming APIs to let developers customize their own WebView instances.

```
WebView.setSupportMultipleWindows(true/false)
```

Security Issues & Concrete Attacks

- WebView customization VS Regular web behaviors

  => Privileged main-frame navigation attack

  - WebView.SupportMultipleWindows = false
  - 

    ```
    window.open("https://attacker.com", "_blank"
    ```

- Iframe sandbox? **No!**

DCV Summary

- WebView UI Redressing Attacks
  - Creation & Closure
- Main-Frame Navigation Attacks
  - Traditional & Privileged

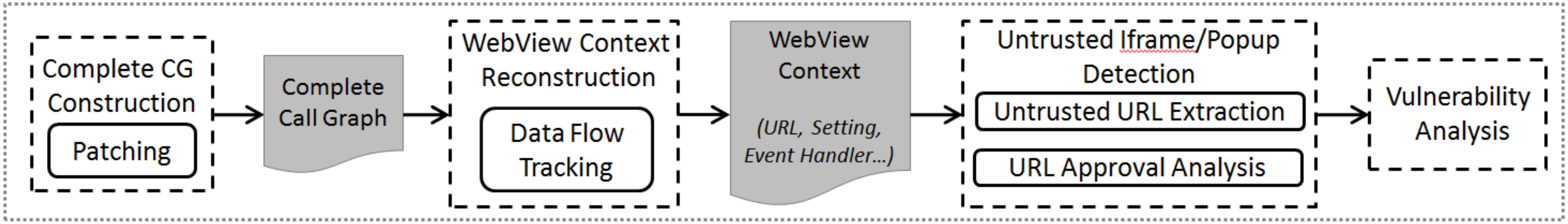
Phishing

- Origin Hiding Attacks → *Stealing privacy & accessing hardware*

- Existing defense solutions are limited to prevent DCV based attacks.

Security Assessment

DCV-Hunter: Automatic Vulnerability Detection



Complete CG Construction

Patching

Complete Call Graph

WebView Context Reconstruction

Data Flow Tracking

WebView Context

(URL, Setting, Event Handler...)

Untrusted Iframe/Popup Detection

Untrusted URL Extraction

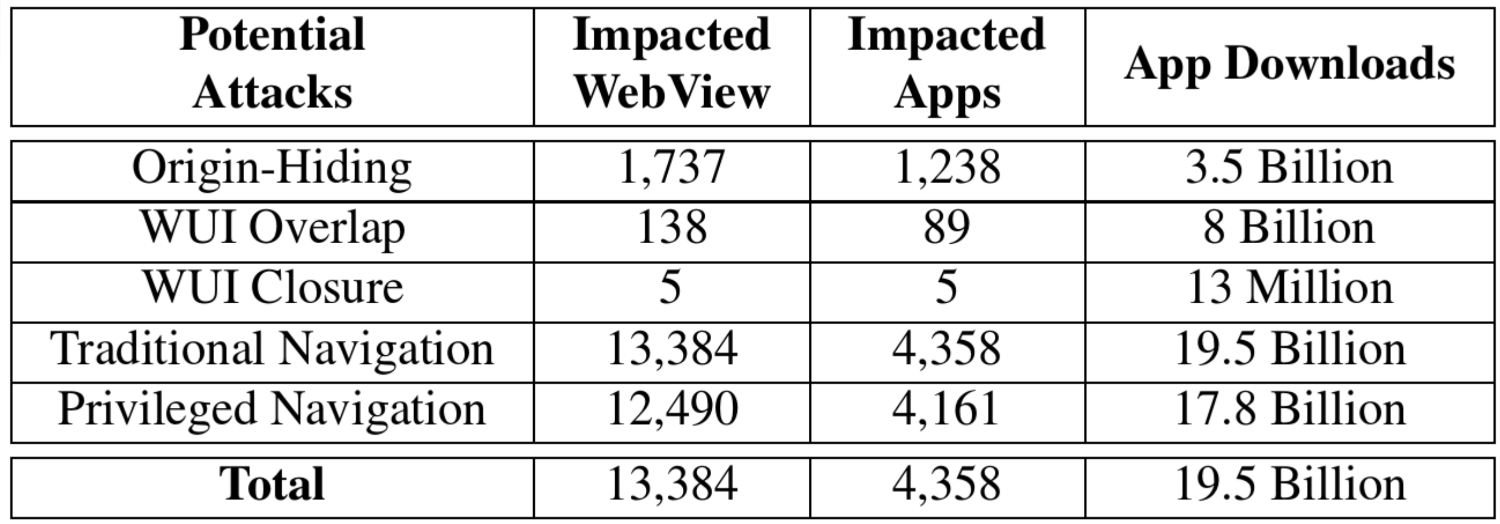
URL Approval Analysis

Vulnerability Analysis

Security Assessment

- Dataset
  - 17K most popular free apps from Google Play
    - = 32 categories X 540 apps for each category
- Result overview
  - 11,341 hybrid apps
  - 4,358 hybrid apps (38.4%) were potentially vulnerable, including
    - 13,384 potentially vulnerable WebView instances and
    - 27,754 potential vulnerabilities
  - 19.5 Billion downloads
- Low false positive

Security Assessment



Potential Attacks	Impacted WebView	Impacted Apps	App Downloads
Origin-Hiding	1,737	1,238	3.5 Billion
WUI Overlap	138	89	8 Billion
WUI Closure	5	5	13 Million
Traditional Navigation	13,384	4,358	19.5 Billion
Privileged Navigation	12,490	4,161	17.8 Billion
Total	13,384	4,358	19.5 Billion

Security Assessment

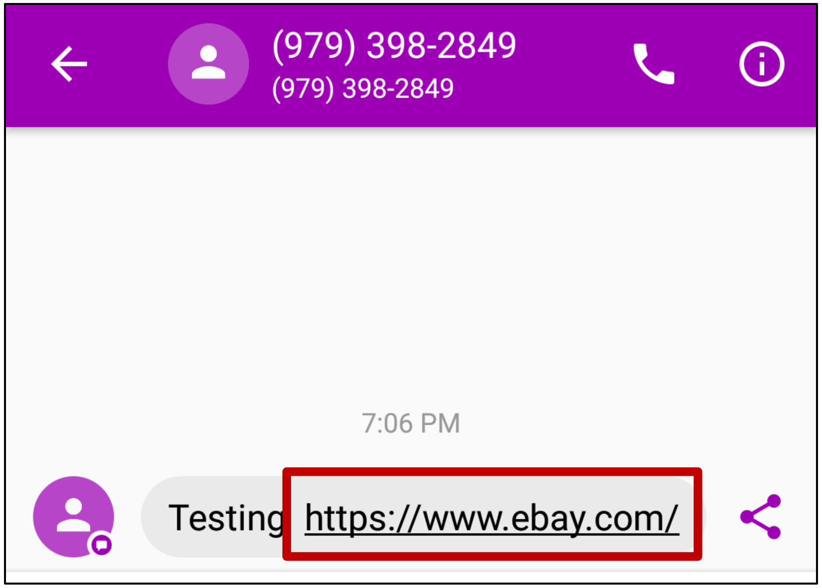
- Many high-profile apps are impacted
  - Facebook, Instagram, Facebook Messenger, Google News, Skype, Uber, Yelp, WeChat, Kayak, ESPN, McDonald's, Kakao Talk, and Samsung Mobile Print
  - Third-party development libraries
    - Facebook Mobile Browser & Facebook React Native
  - Leading password management apps
    - dashlane, lastpass, and 1password
  - Popular banking apps
    - U.S. bank, Huntington bank, and Chime mobile bank

Case Studies

- Facebook Messenger
  - Providing its own address bar?
  - No! pixel & race-condition problems

Case Studies

- Facebook Messenger



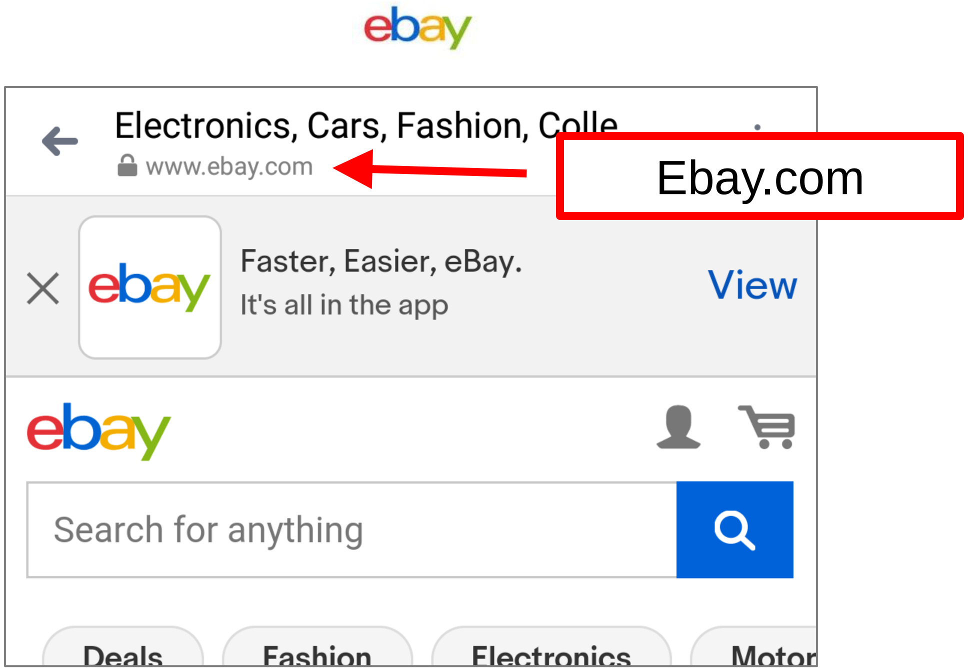
(979) 398-2849
(979) 398-2849

7:06 PM

Testing https://www.ebay.com/

Case Studies

- Facebook Messenger
  - WUI redressing attack



Electronics, Cars, Fashion, Colle

www.ebay.com

Faster, Easier, eBay.
It's all in the app

View

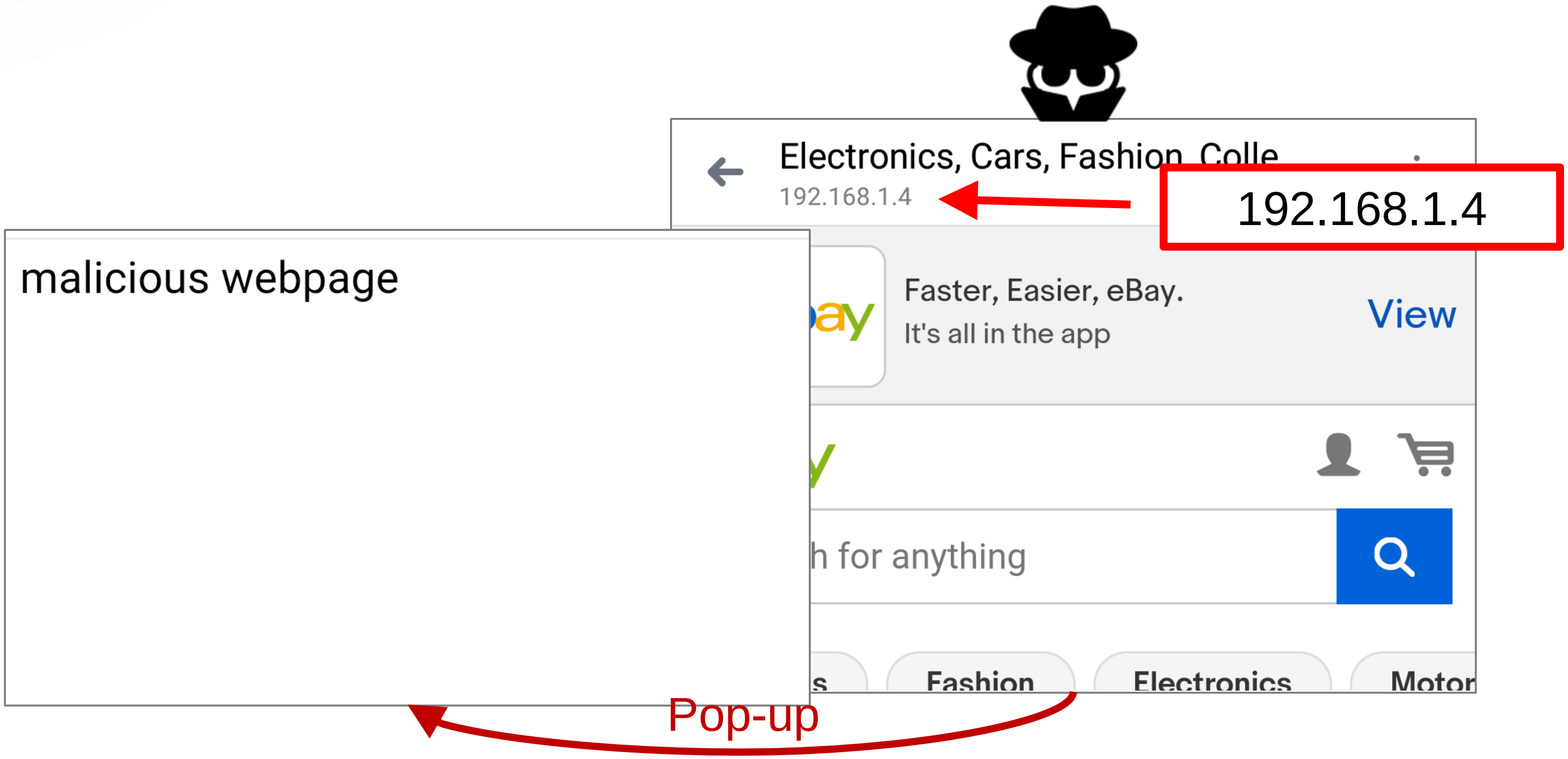
Search for anything

Deals | Fashion | Electronics | Motor

Ebay.com

Case Studies

- Facebook Messenger
  - WUI redressing attack



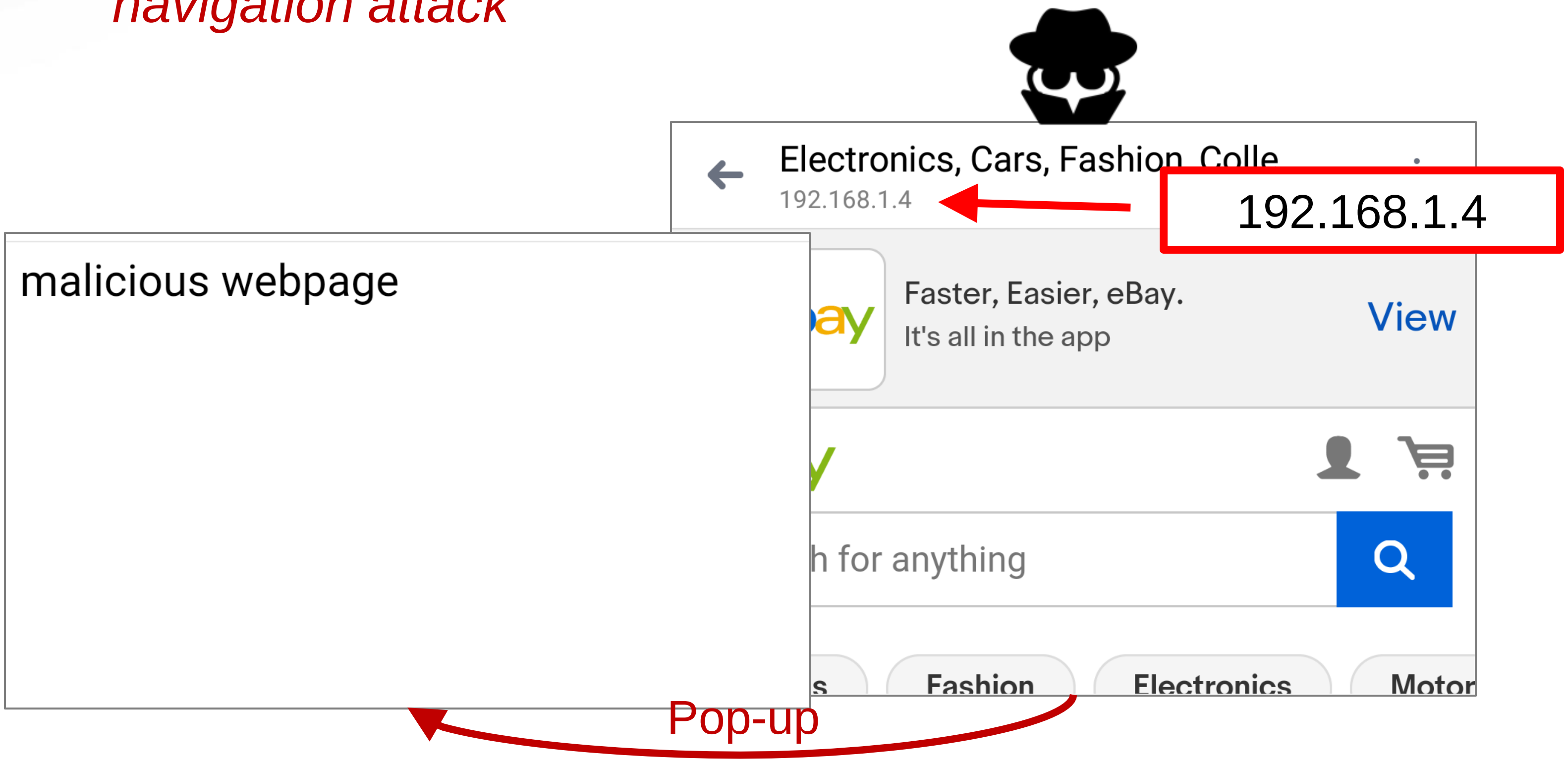
Electronics, Cars, Fashion, Colle
192.168.1.4

Faster, Easier, eBay.
It's all in the app

h for anything

Case Studies

- Facebook Messenger
  - *Blended attack: WUI redressing attack + Traditional navigation attack*



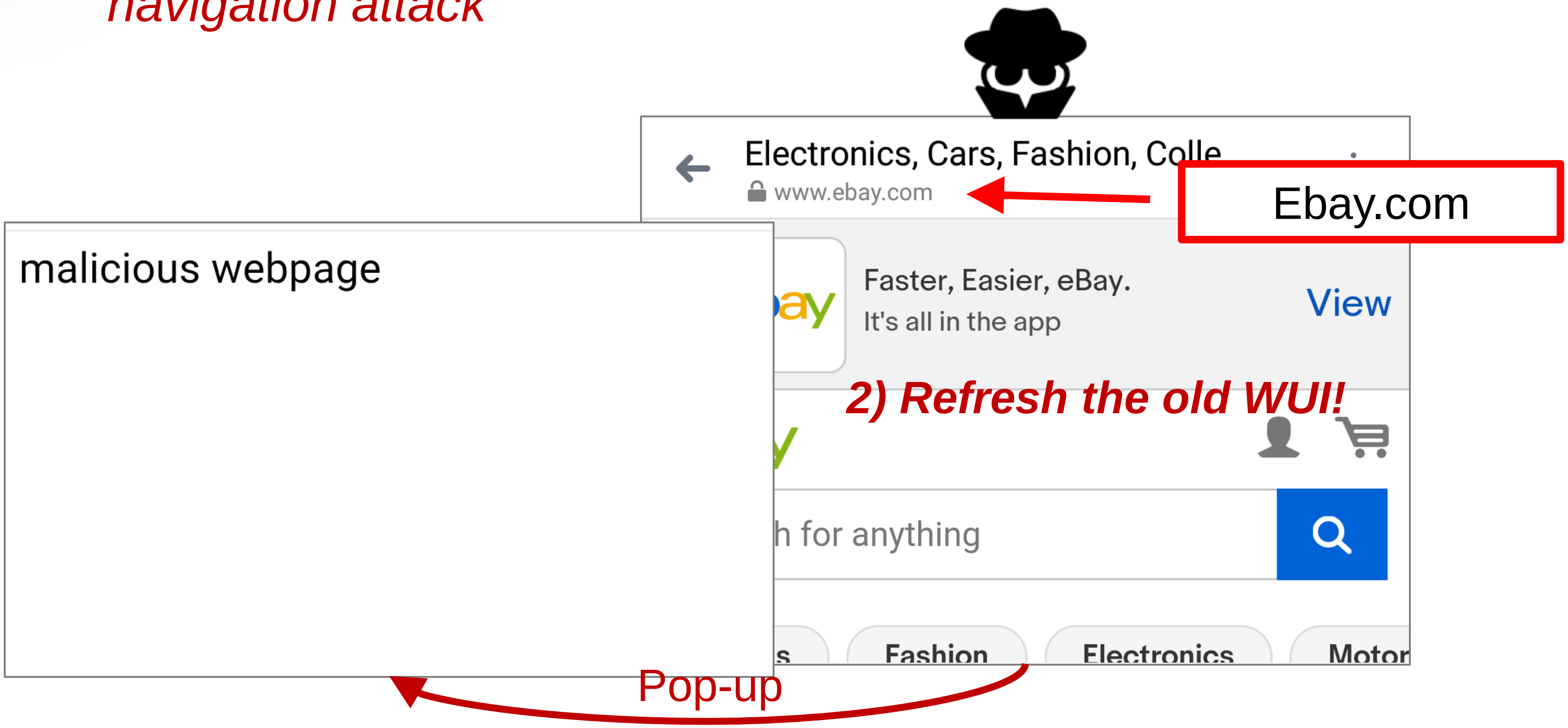
192.168.1.4

malicious webpage

Pop-up

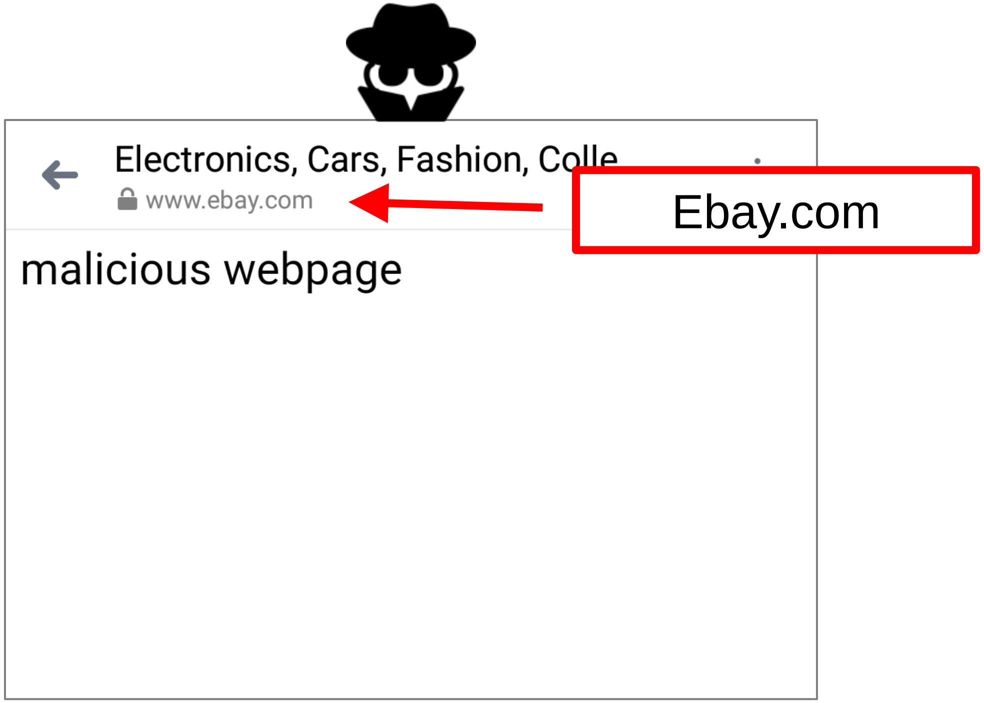
Case Studies

- Facebook Messenger
  - *Blended attack: WUI redressing attack + Traditional navigation attack*



Case Studies

- Facebook Messenger
    - *Blended attack: WUI redressing attack + Traditional navigation attack*



Demos: https://sites.google.com/view/dcv-attacks

DCV Mitigation

DCV Mitigation

- Mitigating the DCV issues from the root (i.e., inconsistencies)
  - Reducing the inconsistencies between browsers and WebView
    - Floating URL address bar
    - Validating sensitive operations (e.g., popup creation)

- Evaluation
  - Our defense solution is
    - Effective
    - Compatible (90% Android devices)
    - Low-overhead

Conclusion

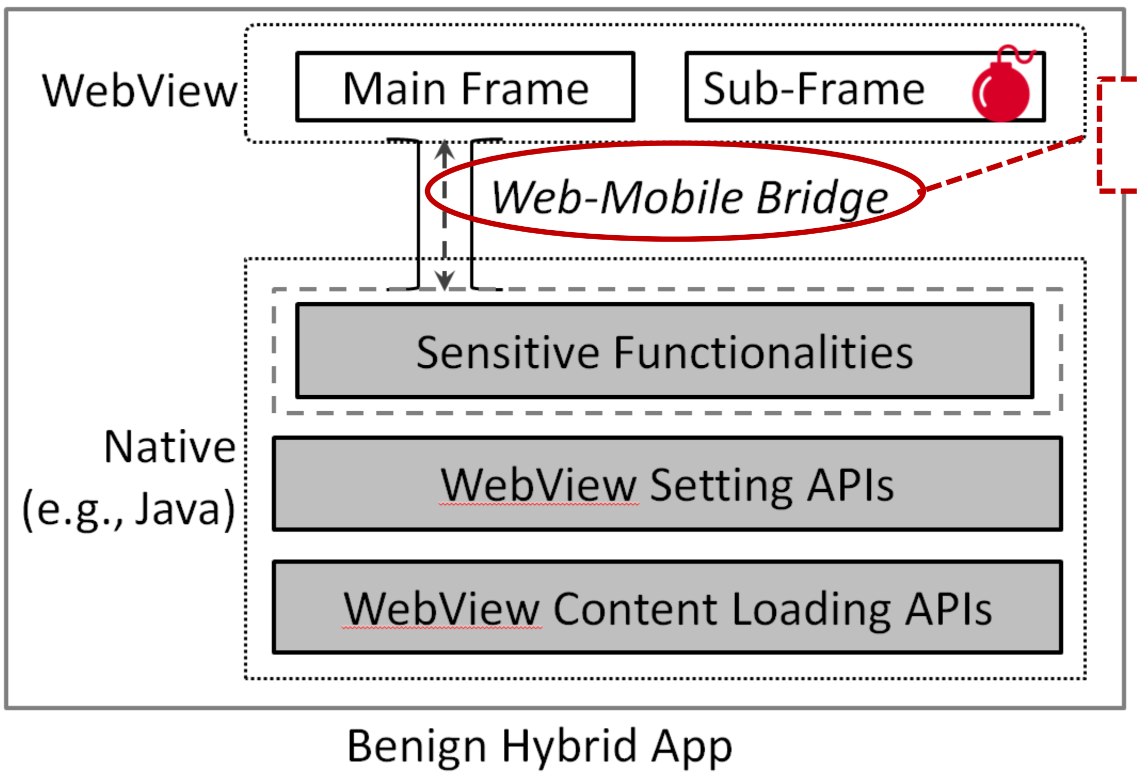
Conclusion

- WebView attracted more and more attention.
- Iframe/popup behaviors were well studied in regular browsers, but rarely understood in the new web environment of WebView.
- We filled the gap by identifying a novel class of vulnerabilities (DCVs), assessing the security impacts with a novel detection tool (DCV-Hunter), and mitigating the DCV issues with a multi-layer defense solution.

Thanks!

Inconsistencies Between Browsers and WebView

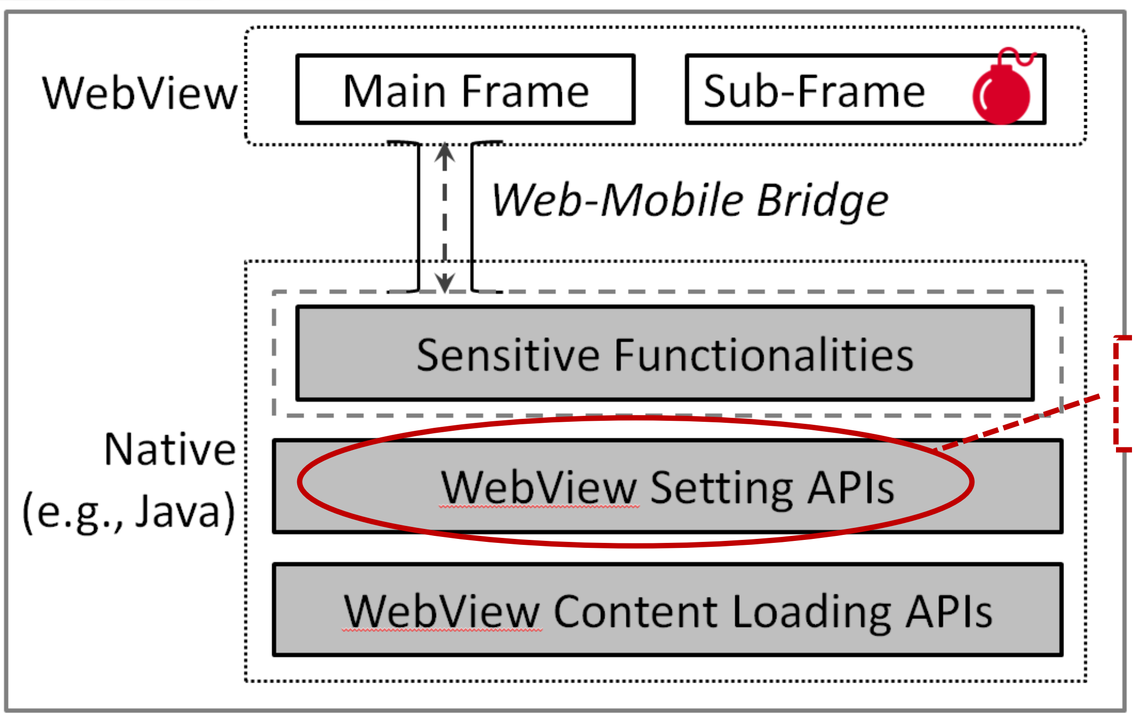
- Programming features



Android.Sensitive-Function()

Inconsistencies Between Browsers and WebView

- Programming features

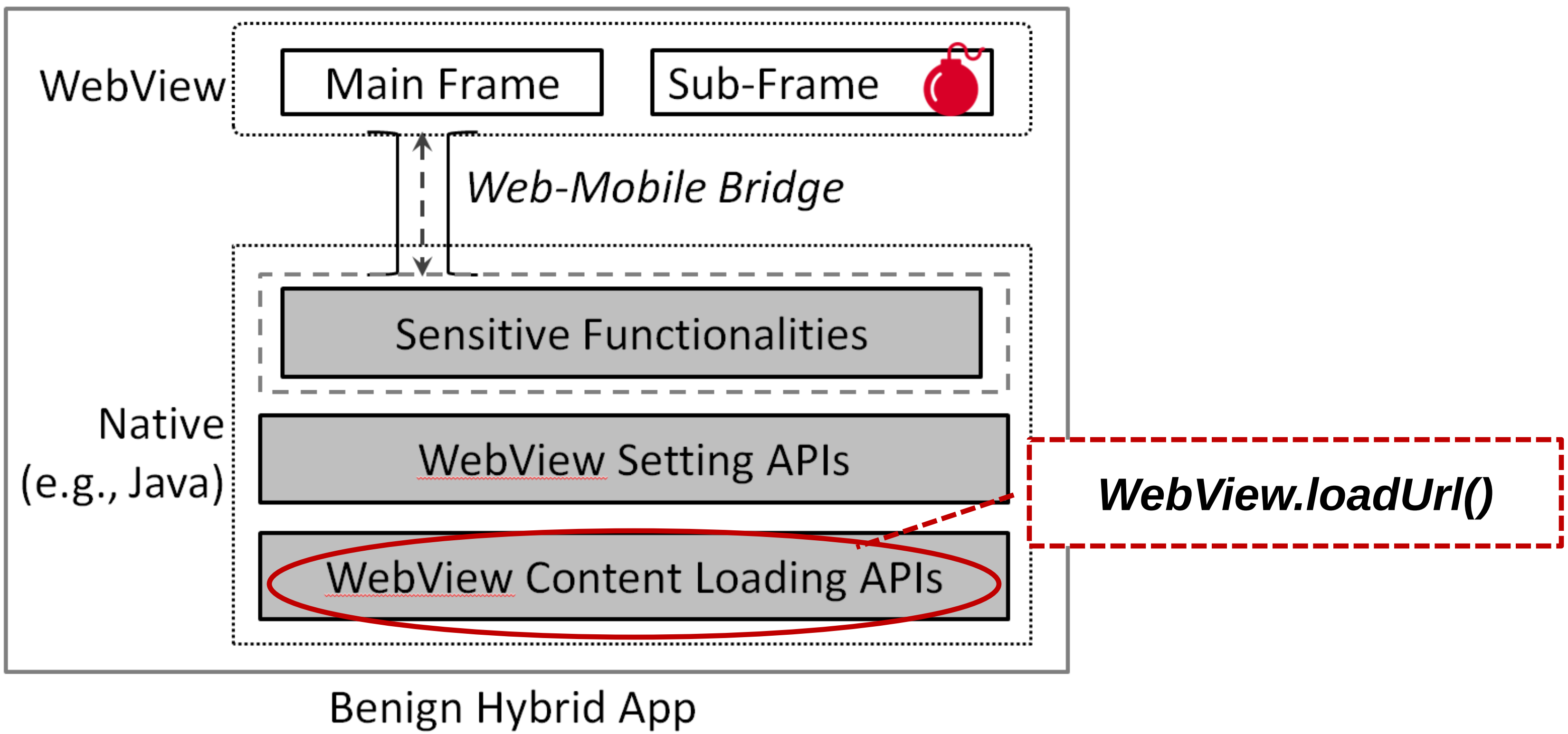


WebView.Support-MultipleWindow()

Benign Hybrid App

Inconsistencies Between Browsers and WebView

- Programming features


WebView
Main Frame
Sub-Frame
Web-Mobile Bridge
Sensitive Functionalities
Native
(e.g., Java)
WebView Setting APIs
WebView Content Loading APIs
WebView.loadUrl()
Benign Hybrid App