Measuring the Insecurity of Mobile Deep Links of Android

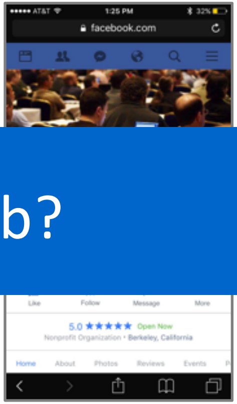
Fang Liu, Chun Wang, Andres Pico, Danfeng Yao, **Gang Wang**

VirginiaTech
Invent the Future

Web Browsing is Going Mobile

- Users spend more time on mobile devices[1]
  - Mobile devices ~ 3.1 hours
  - Laptops/Desktops ~ 2.2 hours

- Native apps: the new web interface
  - Shorter loading time



Apps are the future of the web?

[1] Mary Meeker, Internet Trends 2017 - Code Conference, KPCB, 2017

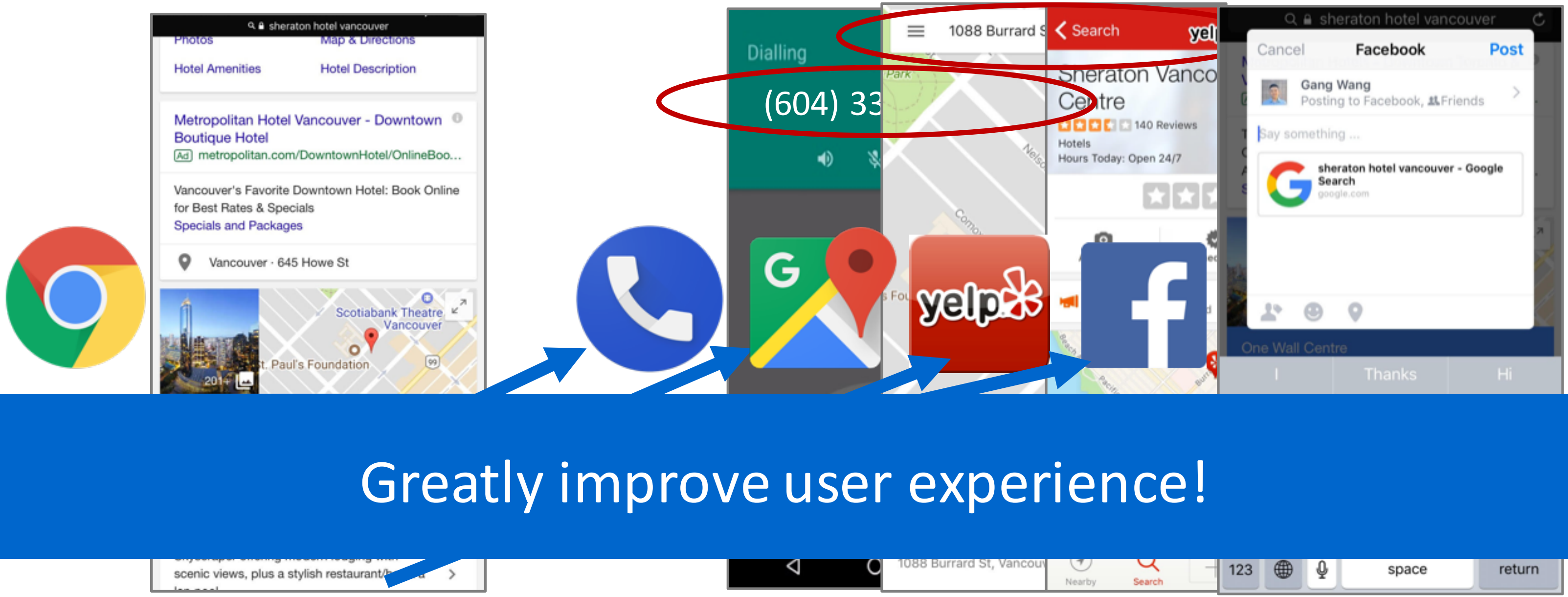
Apps vs. Mobile Websites

- Apps cannot replace websites yet
  - Apps sit in a "walled garden"
  - Difficult to navigate across apps
  - Difficult to search and access in-app content globally

- Apps + mobile websites eco-system
  - Complementary to each other
  - Likely to co-exist (for a long time)

Web-App Communication via Deep Links

- Deeper integration of websites and apps
  - Mobile deep links: URIs pointing to pages inside apps



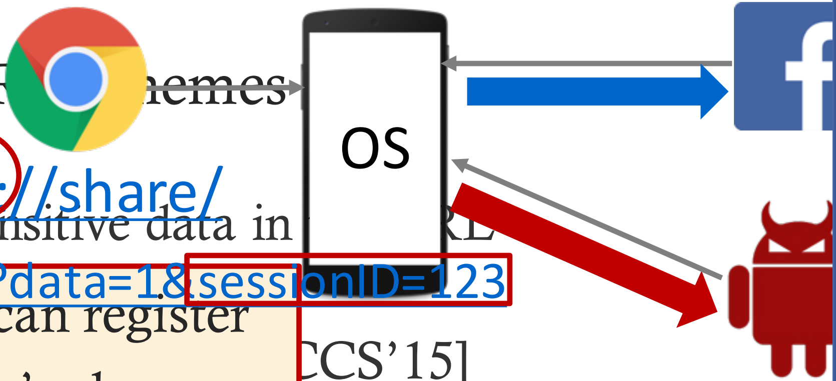
Greatly improve user experience!

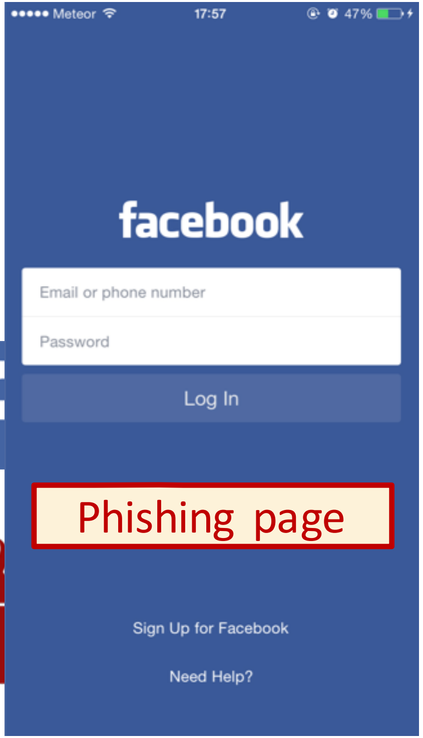
Hijacking Risks of Deep Links

- Scheme URL: mobile deep link v1.0
  - Designed for functionality, no security features
  - Apps can register their own scheme to the OS
  - Android and iOS since 2009

- Hijacking UR hemes
  - Phishing
  - Stealing sensitive data in RL
  - CCS'15]

Any app can register other apps' schemes





facebook

Email or phone number

Password

Log In

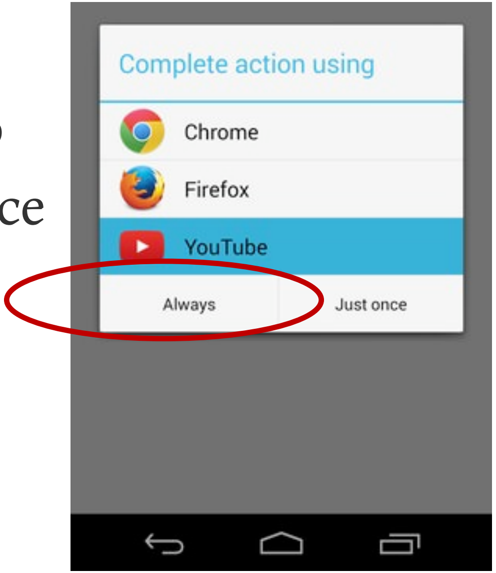
Phishing page

Sign Up for Facebook

Need Help?

Defense Relying on Users

- Prompt users when multiple apps have the same scheme
- But, user prompting can be skipped
  - If the malicious app installed before the real app
  - If the malicious app tricked users to set preference
- User as the only defense = bad defense



Deep Link v2.0 Prevents Link Hijacking

- App links
  - HTTP/HTTPS links only, no custom schemes
  - Requires app link association

~~fb://~~ ➔ https://facebook.com/

- Intent URL
  - Explicitly specify the target app by package name

~~fb://~~ ➔
intent://p#Intent;scheme=fb;package=com.facebook;end

Uniqueness guaranteed by the app market

This Study

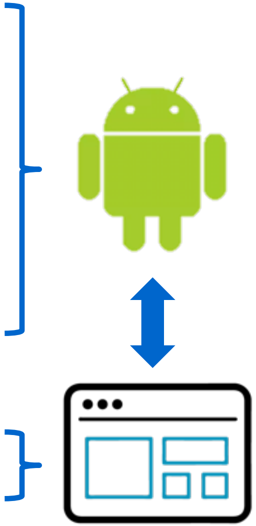
- Research questions
  - How are different mobile deep links used in practice?
  - How likely is an app's scheme hijacked by another app?
  - How effective are the new deep link mechanisms in mitigating the hijacking threats?

- Large-scale empirical measurements
  - Deep links across web and apps
  - Primarily focus on Android (>80% market share)

Let the DATA speak

Outline

- ~~Introduction~~
- The Adoption of Mobile Deep Links
  - Scheme URL vs. App Link
  - App Links: Vulnerabilities & Misconfigurations
- Characterizing Hijacking Attacks
- Hijacking Threats on the Web



Datasets

- Android apps (25 app categories)
  - 164,322 most popular apps, December 2014
  - 164,963 most popular apps, August 2016
  - 115,399 apps in both snapshots

Register the same link?

- Popular websites
  - Alexa top 1 million domain's index page, October 2016
  - Dynamic crawler to mimic Chrome mobile browser (OpenWPM[1])
  - Lower bound of mobile deep links on the web

Hijacked links on the web pages?

[1] ENGLEHARDT, S., AND NARAYANAN, A. Online tracking: A 1-million-site measurement and analysis. In *Proc. of CCS* (2016)

Deep Link Usage in Apps

Dataset	Total Apps	Apps register Scheme URLs	Apps register App Links	Apps register either Links
2014	164,322	10,565 (6.4%)	4,545 (2.8%)	12,428 (7.6%)

~90% growth rate in deep link adoption

Are App links properly verified?

Key observations

- Mobile deep links are getting popular among apps
- The vulnerable scheme URLs are still increasinly used

App Link Verification

- App link association to prevent link hijacking

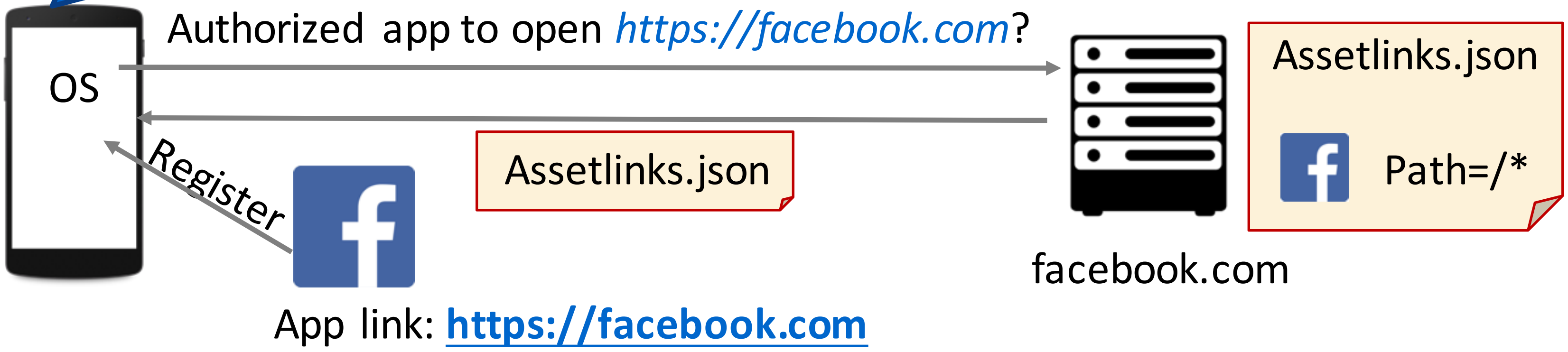
ved

e App link and the web domain

“universal link”

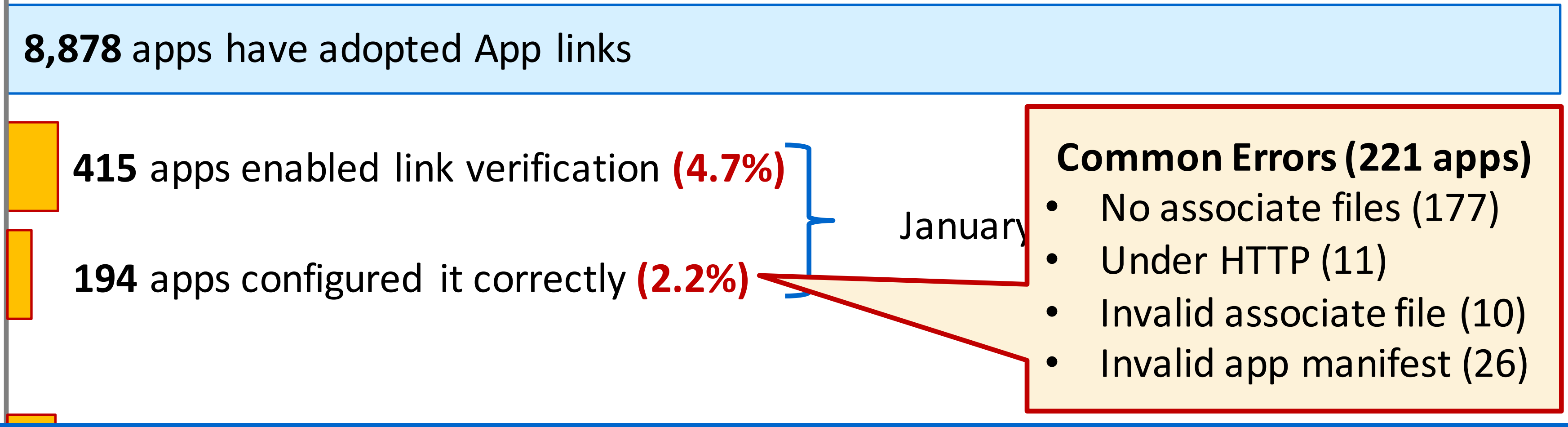
Unverified links

- Android: still works, but trigger user prompt
- iOS: cannot open the link in the app



OS
Authorized app to open *https://facebook.com*?
Register
Assetlinks.json
Assetlinks.json
Path=/*
facebook.com
App link: **https://facebook.com**

App Link Verification in Practice



8,878 apps have adopted App links

415 apps enabled link verification **(4.7%)**

194 apps configured it correctly **(2.2%)**

January

Common Errors (221 apps)

- No associate files (177)
- Under HTTP (11)
- Invalid associate file (10)
- Invalid app manifest (26)

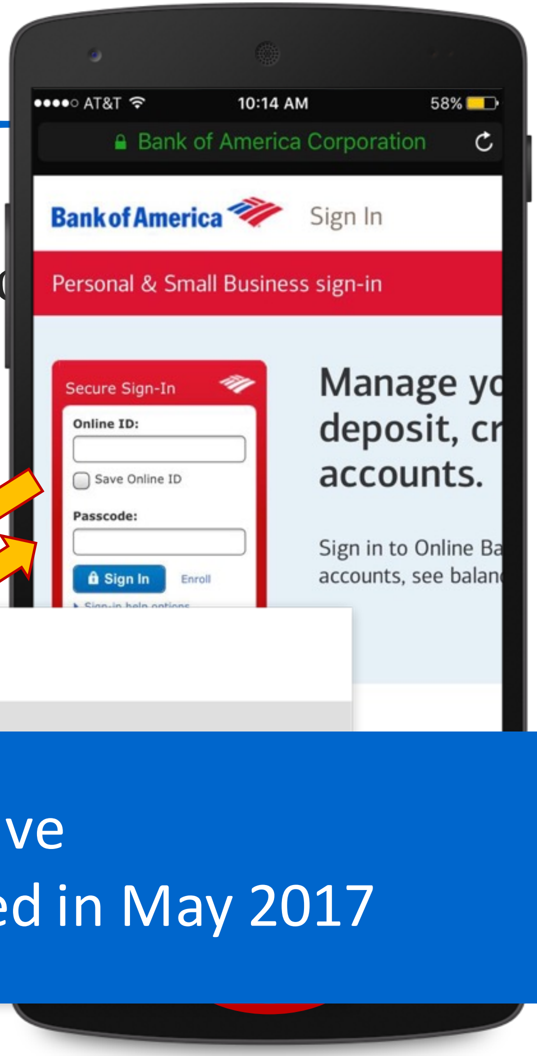
- Rarely do apps verify their App links correctly
  - A lack of incentives: unverified App links can still open apps
- Configuration errors are not identified and mitigated quickly

App Link Vulnerability: Over-

- Allows unverified app links to skip user pr

  links that

- Hijack password without user knowledge!
- HTTPS does not help



https://recipe.com/cupcake

Manifest.xml
Intent filters
Open with

- Root cause: the preference setting is too excessive
- Reported to Google in Feb 2017, case established in May 2017

Outline

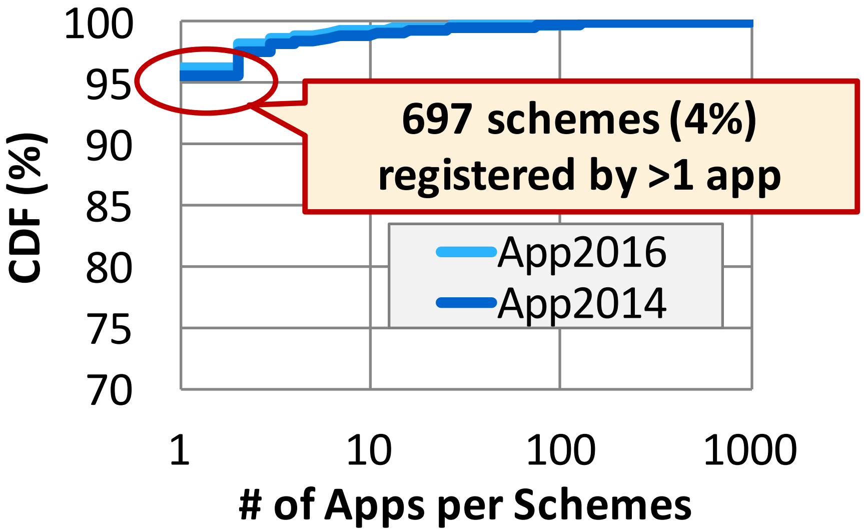
- ~~Introduction~~
- ~~The Adoption of Mobile Deep Links~~
-

- Scheme URLs are still widely used
- App links are rarely verified correctly
- App links introduce a new vulnerability

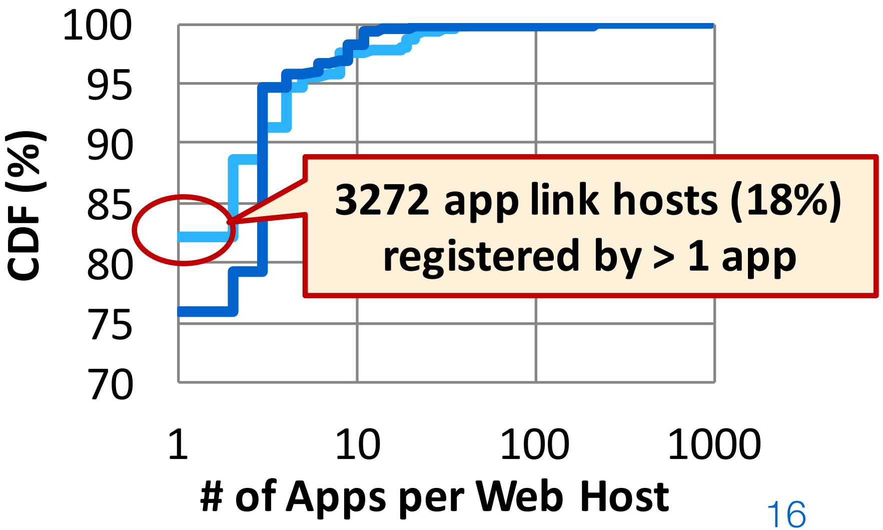
- Hijacking Threats on the Web

Identifying Potential Hijacking Apps

- Link collision: multiple apps that registered the same Link
  - 18,839 unique schemes (e.g., fb://)
  - 18,561 unique App link hosts (e.g., facebook.com)



697 schemes (4%) registered by >1 app



3272 app link hosts (18%) registered by > 1 app

Classifying Link Collisions

Not all link collisions are malicious

Scheme URL

Functional scheme

Represents a common functionality
e.g. **geo://, tel://, file://**

Third-party scheme

Used by 3rd-party library and APIs
e.g., **x-oauthflow-twitter://**

Per-app scheme

Represents individual apps
e.g., **fb://, twitter://**

App Link

~~**Functional web host**~~

N/A

Third-party web host

e.g., **zxing.appspot.com**

Per-app web host

e.g., **facebook.com, twitter.com**

Potentially Malicious Hijacking

Classifying Per-App Hijacking

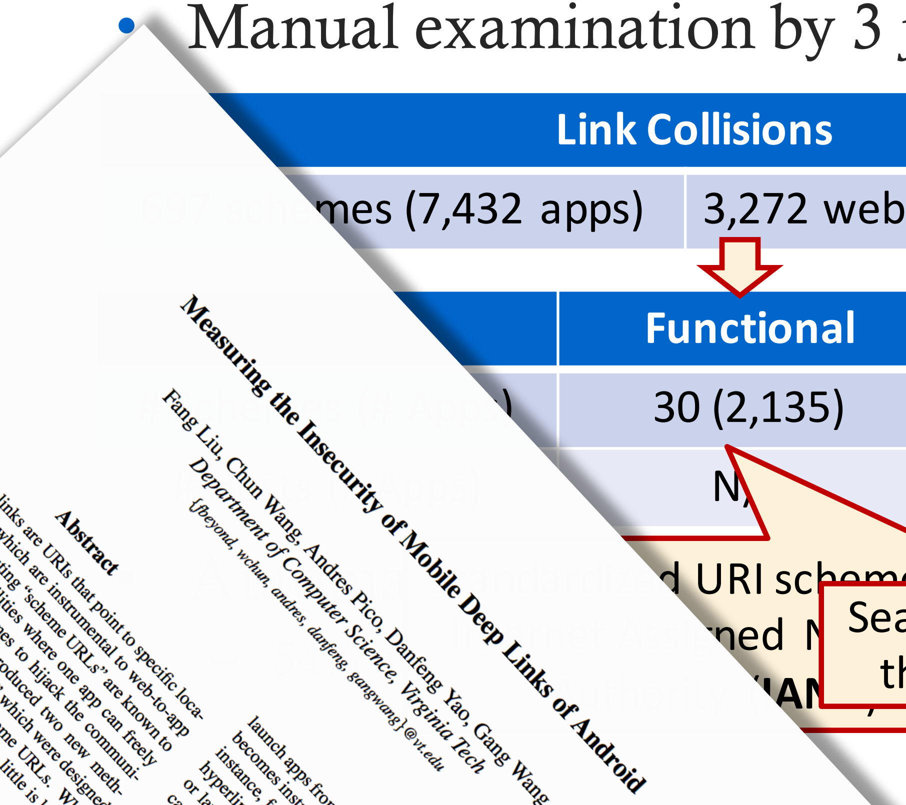
- Manual examination by 3 judges

Link Collisions	
697 schemes (7,432 apps)	3,272 web hosts (2,868 apps)

	Functional	3rd-party	Per-app
# Schemes (# Apps)	30 (2,135)	197 (3,972)	149 (893)
[illegible] (# Apps)	N/	137 (999)	2,314 (1,593)

Search for online the 3rd-party libs and APIs

Not from the same developer



Measuring the Insecurity of Mobile Deep Links of Android

Fang Liu, Chun Wang, Andres Pico, Danfeng Yao, Gang Wang
Department of Computer Science, Virginia Tech
{fbeyond, wchun, andres, danfeng, gangwang}@vt.edu

Abstract

links are URIs that point to specific loca- which are instrumental to web-to-app ting "scheme URLs" are known to lities where one app can freely es to hijack the communi- oduced two new meth- which were designed me URLs. W little is

launch apps fro becomes inst instance, f hyperli or la

18

Hijacking Case Studies

Google Google Maps

- Traffic hijacking
  - **google.com** registered by 480 apps (305 non-Google developers)
  - **google.navigation://** registered by 79 apps (32 developers)
  - Other popular targets facebook airbnb YouTube tumblr.

- Competing Apps
  - Careem (5M downloads)

    widely integrated with hotel websites/apps
  - QatarTaxi (10K downloads)

    also registered **careem://***

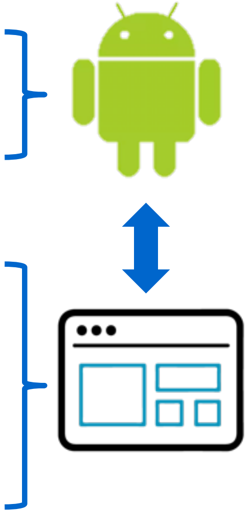
Case Studies (Cont.)

- Redirection apps and MITM
  - Resolve deep links and redirect users to target apps
  - Hard-coded mapping, without permission of the target app
  - Log URL and parameters to files

- Example: URLLander
  - Registered payments.ebay.com while the official eBay app did not
  - Registered www.paypal.com (SESSIONID parameter)

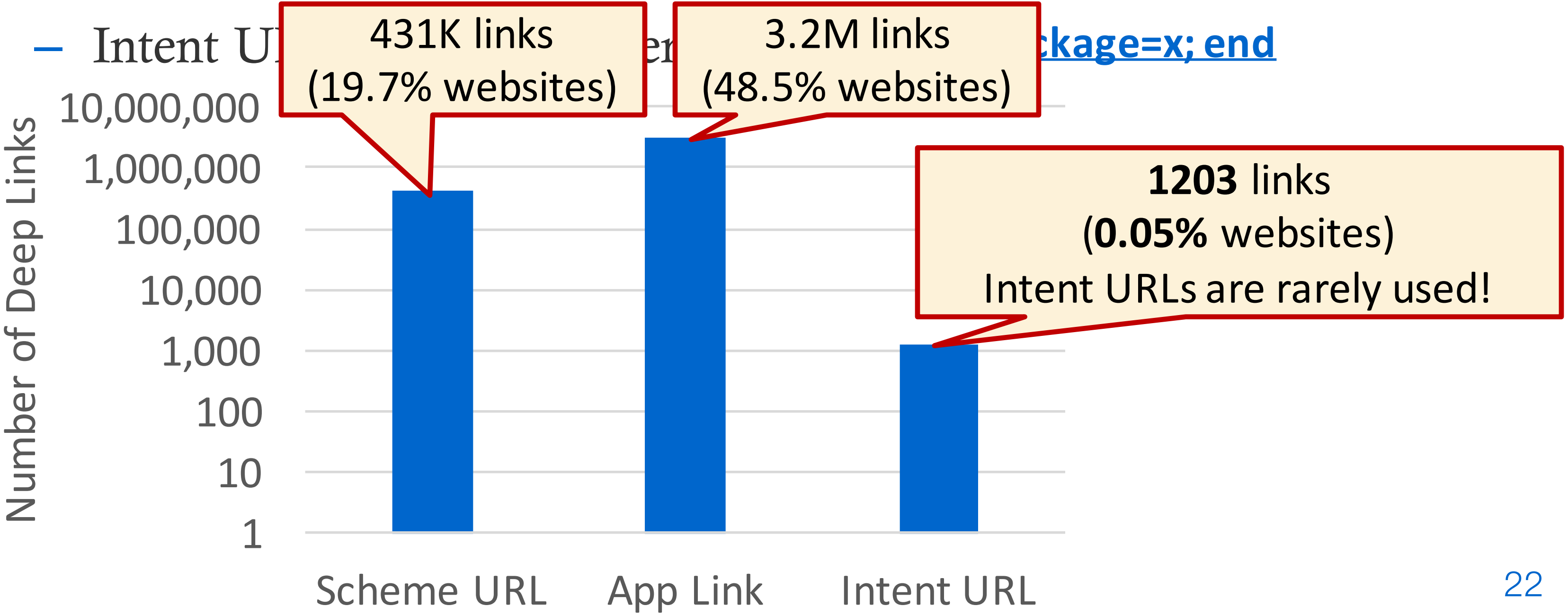
Outline

- ~~Introduction~~
- ~~The Adoption of Mobile Deep Links~~
- ~~Characterizing Hijacking Attacks~~
- Hijacking Threats on the Web
  - Usage of Intent URL
  - Hijacked App Links vs. Scheme URLs



Deep Links on Alexa Top 1M Websites

- Extracting deep links from web pages
  - Regular expression matching with scheme URLs/App links
  - Intent U er **ckage=x; end**



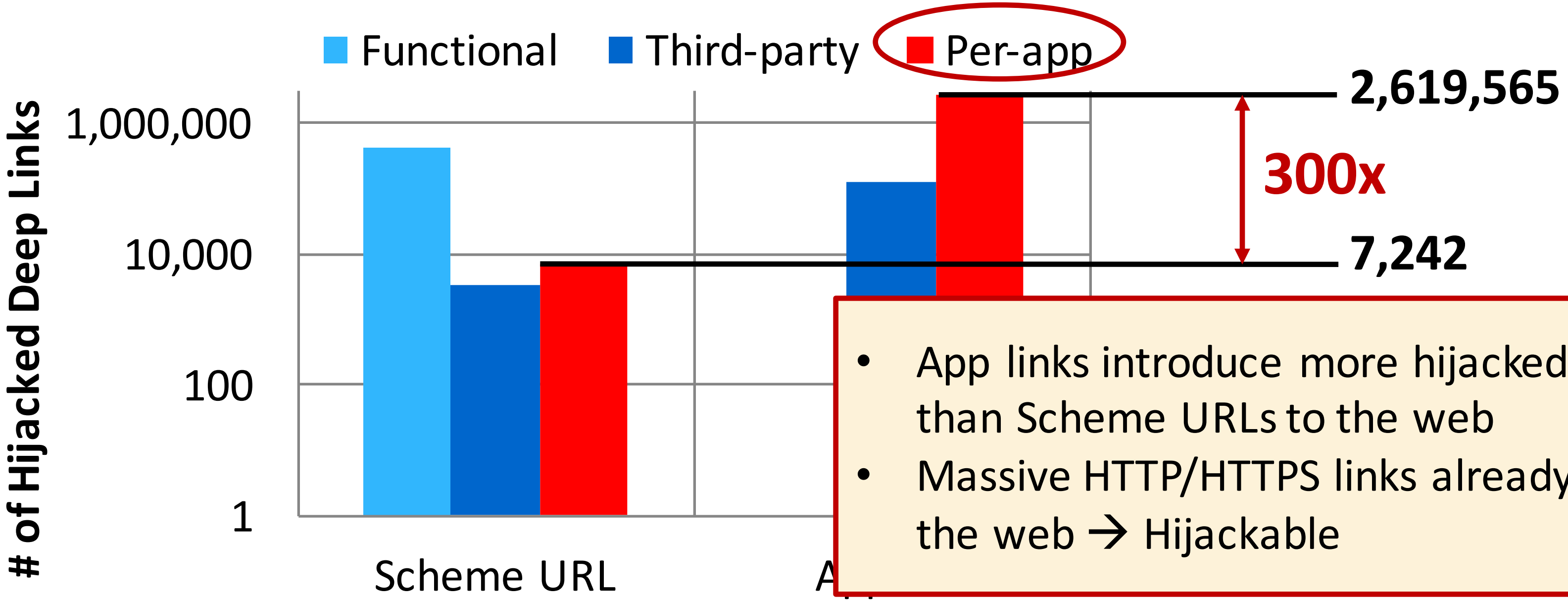
431K links (19.7% websites)

3.2M links (48.5% websites)

1203 links (**0.05%** websites) Intent URLs are rarely used!

“Hijacked” Deep Links on the Web

- Deep links on the web that may take users to the wrong app
  - Deep links registered by multiple apps vs. links on the web pages



- App links introduce more hijacked links than Scheme URLs to the web
- Massive HTTP/HTTPS links already exist on the web → Hijackable

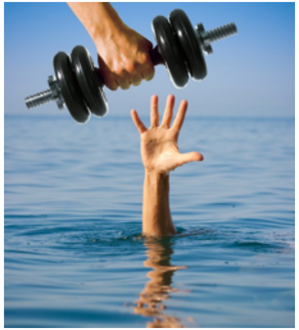
Discussion

- Scheme URLs are still widely used by apps and websites

- The new App link not only fails to improve security, but significantly increases hijacking risks
  - App links are rarely verified (2.2% apps did it correctly)

iOS App links: 1,925 out of 12,570 (**15%**) apps have misconfigured the verification

heme URLs



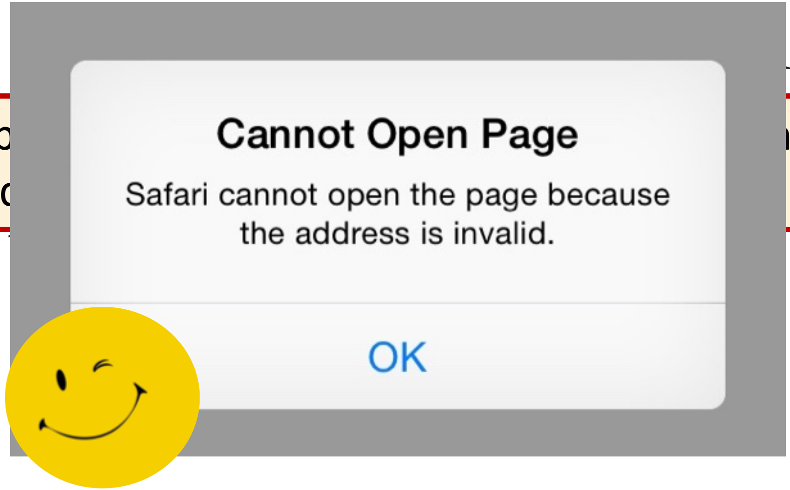
- Intent URLs are rarely used on the web

Countermeasures

- Disable per-app scheme
  - Whitelist functional schemes
- Enforce App link verification
- Fix App link over-permission
  - Set it to the link/domain level

- Break legacy links on the web
- s

[1]Ab ng
And


Cannot Open Page

Safari cannot open the page because the address is invalid.

[1] https://developer.android.com/about/dashboards/index.html

Thank You