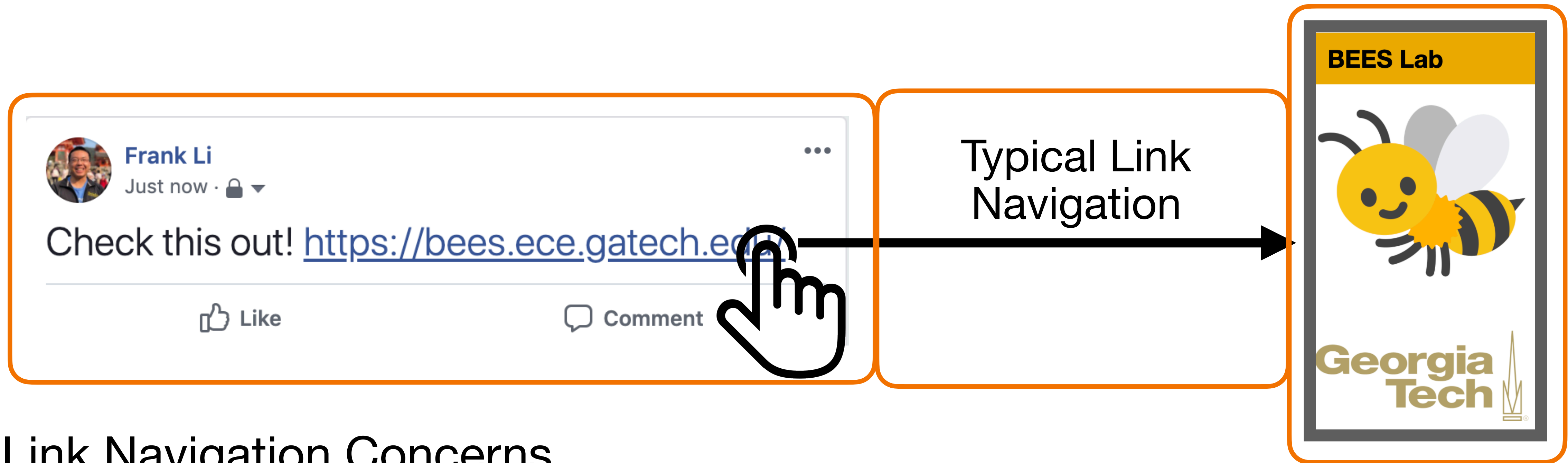


Evaluating the Security & Privacy Contributions of Link Shimming in the Modern Web

Frank Li



Link Navigations

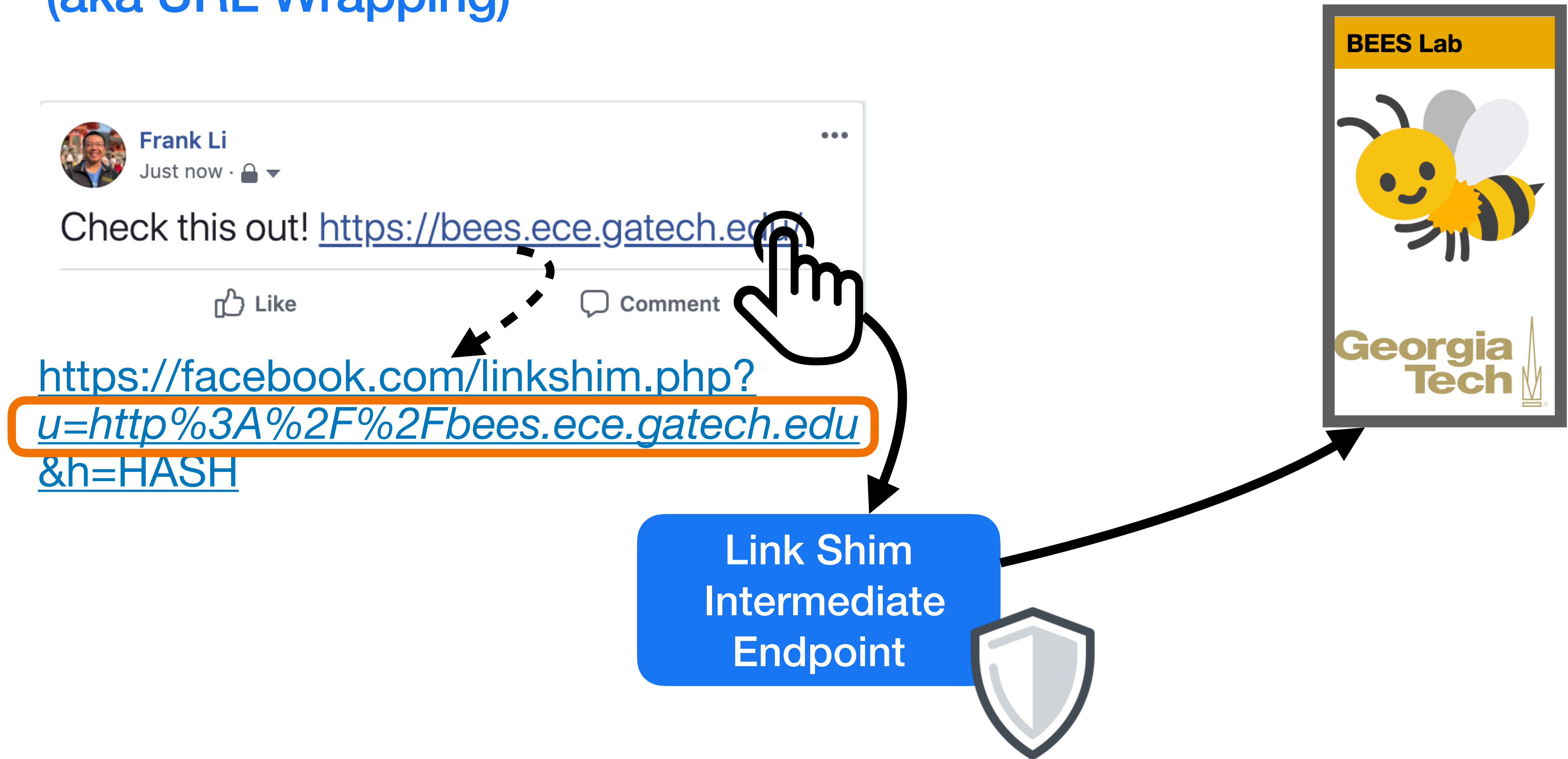


Link Navigation Concerns

1. May leak navigation *source* (via HTTP Referer)
2. Navigation *protocol* may be less secure (HTTP when HTTPS is available)
3. Navigation *destination* may be dangerous (e.g., malware, phishing, spam)

Link Shimming

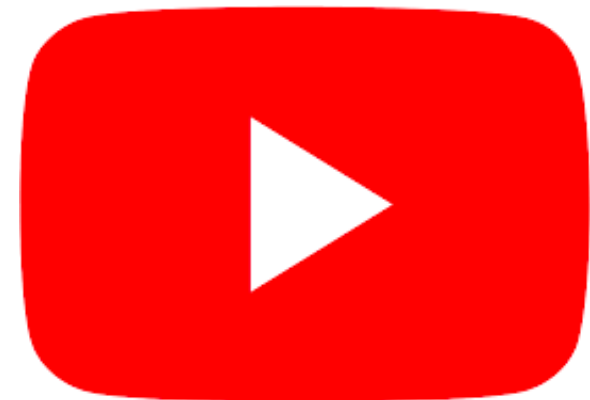
(aka URL Wrapping)



Link Shimming

(aka URL Wrapping)

Used by popular online services for over a decade



Link Shimming

(aka URL Wrapping)

Used by popular online

What are the security & privacy contributions
in the modern web?



Link Shimming vs Modern Web



Navigation Concern	Link Shimming	Modern Web

Link Shimming vs Modern Web



Navigation Concern	Link Shimming	Modern Web
Navigation Source	Referrer = Link Shim Endpoint	Referrer control via HTML or HTTP Headers (rel=noreferrer or Referrer Policy)

Link Shimming vs Modern Web



Navigation Concern	Link Shimming	Modern Web
Navigation Destination	Warning Page (may allow clickthrough)	Browser Warnings (e.g., Google Safe Browsing)


Data Set

Analyzed 1 month of Facebook data on:

1) Link shim navigations (6B)

- Timestamp
- Link shim actions
- Browser Client Differentiation
- Browser Client Characteristics

2) Warning Clickthroughs (300M)




Possible problem with this link

We have detected that this link: **http://EVIL_WEBSITE_EXAMPLE** may be malicious.

To keep your account and device secure, only follow links you trust.

[◀ Go back](#) [➔ Follow link](#)



Leaving Facebook

We're just checking that you want to follow a link to this website:
http://FINAL_DESTINATION_SITE

[◀ Go back](#) [➔ Follow link](#)

Navigation Source Privacy

3 Classes of Browser Clients

Fully Legacy

No HTTP Referer privacy mechanisms

Link shimming improves referrer privacy

Partially Legacy

Supports only rel=noreferrer

Link shimming provides different privacy/ functionality tradeoff

Modern

Supports ReferrerPolicy

Link shimming is not needed *for source privacy*

Navigation Source Privacy

Analyzed fraction of link shim browser clients within each class



**Fully
Legacy**

2%

2%

42%

1%

1%

31%

2%

13%

**Partially
Legacy**

9%

19%

0%

0%

21%

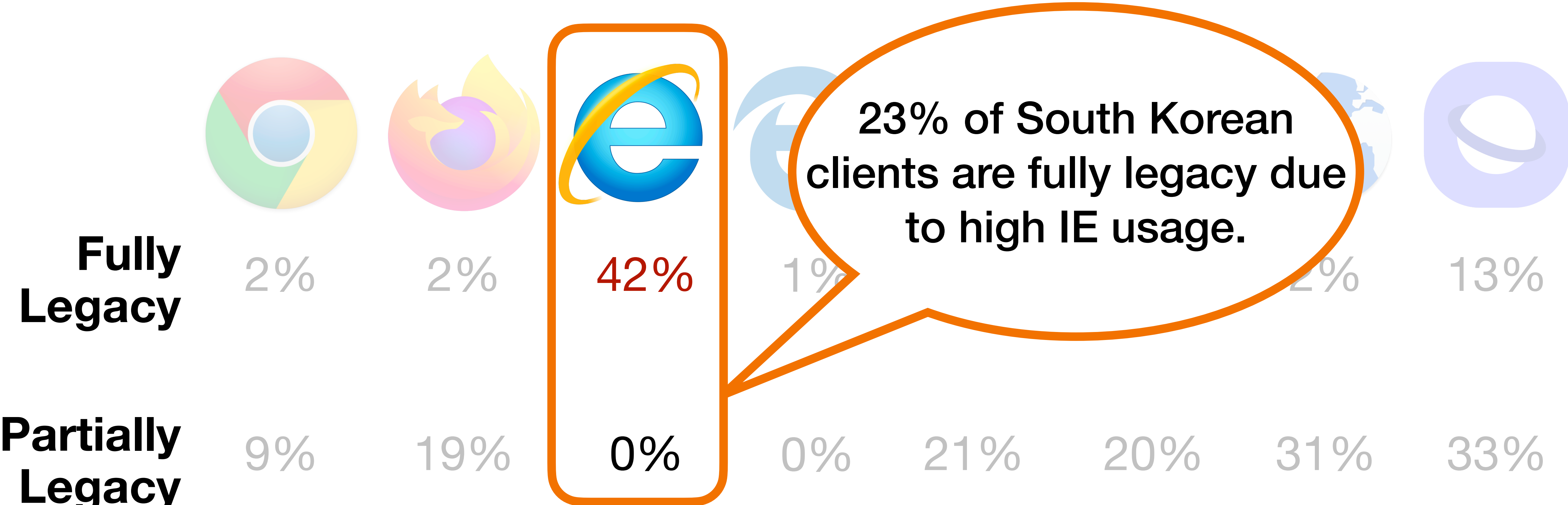
20%

31%

33%

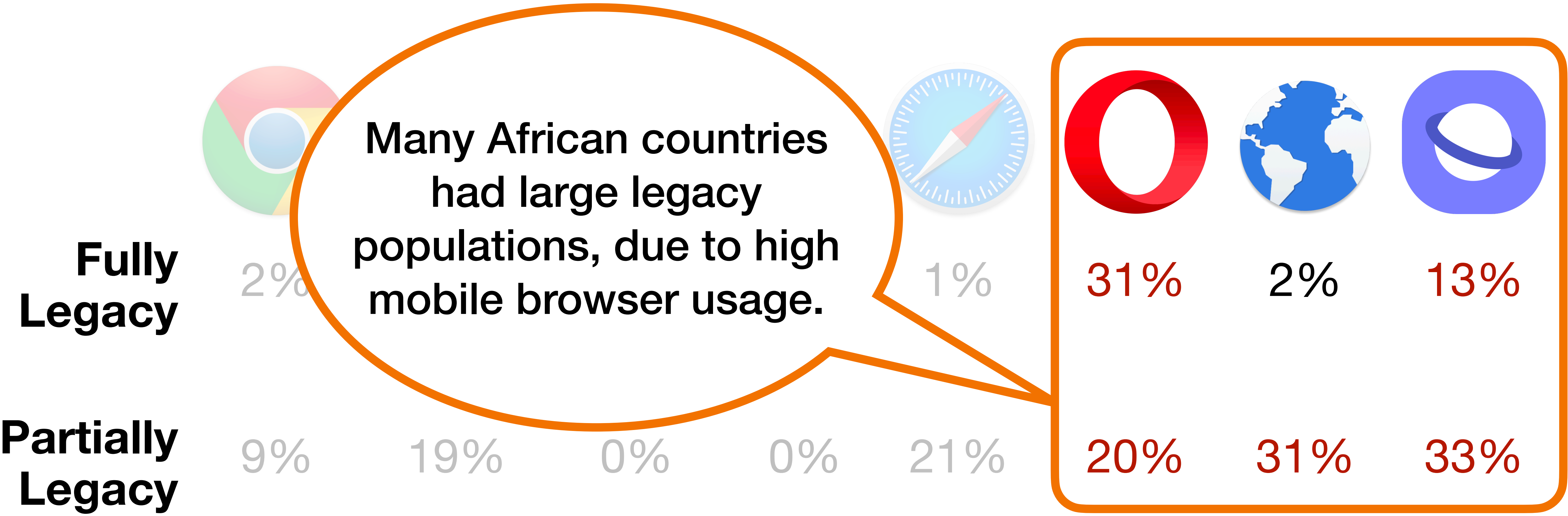
Navigation Source Privacy

Analyzed fraction of link shim browser clients within each class



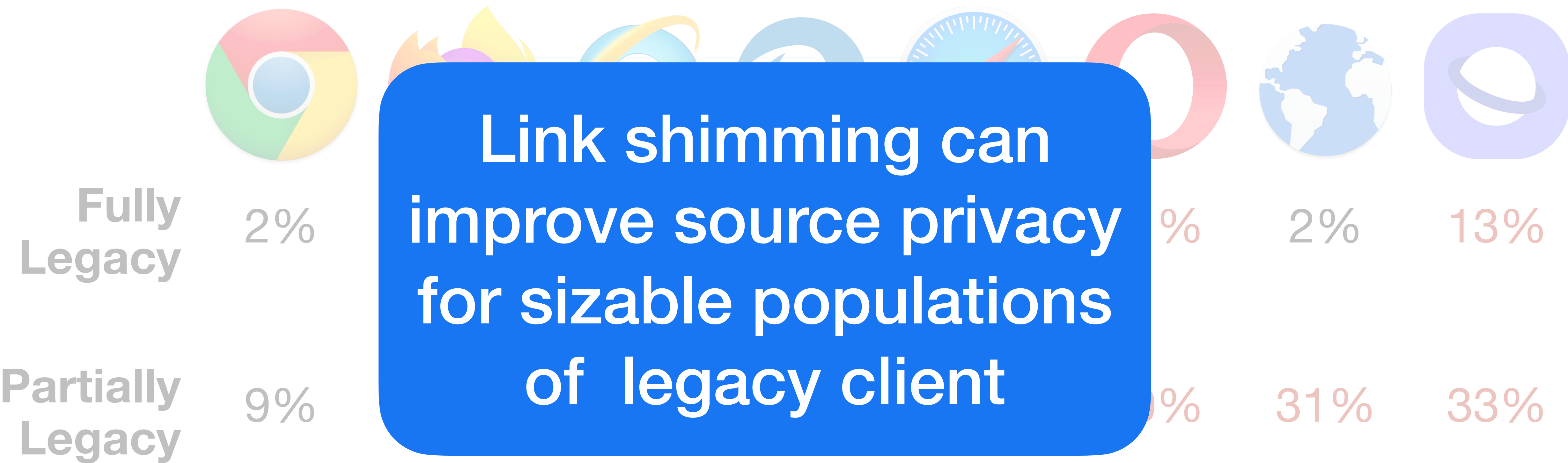
Navigation Source Privacy

Analyzed fraction of link shim browser clients within each class



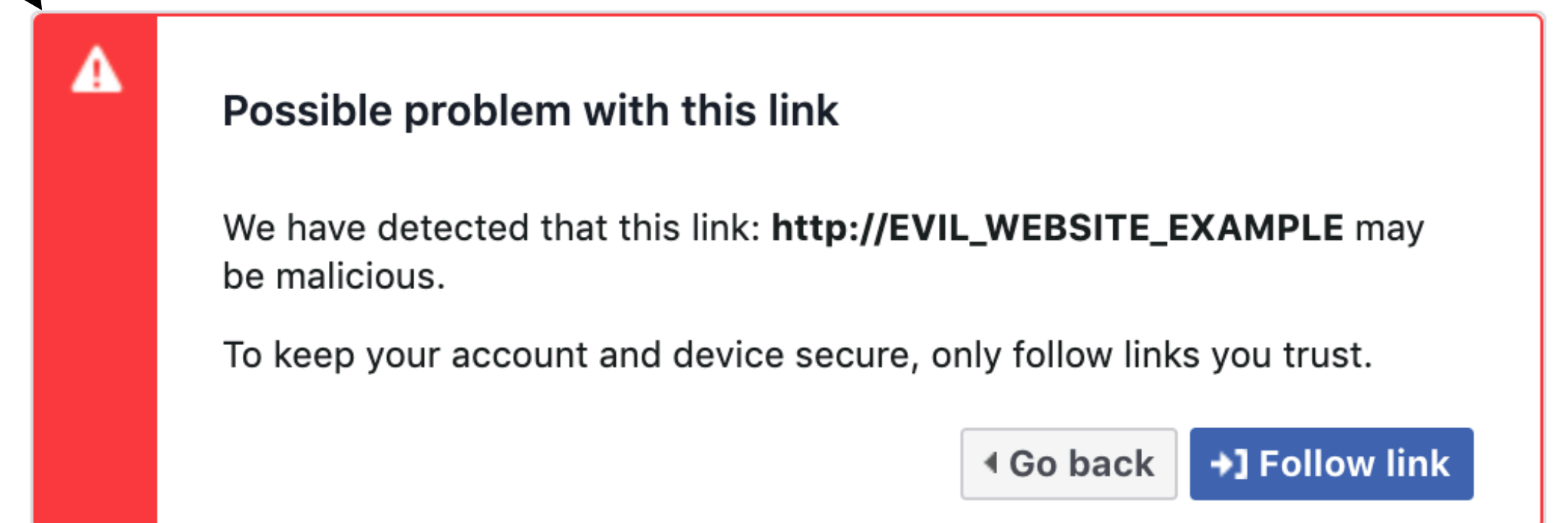
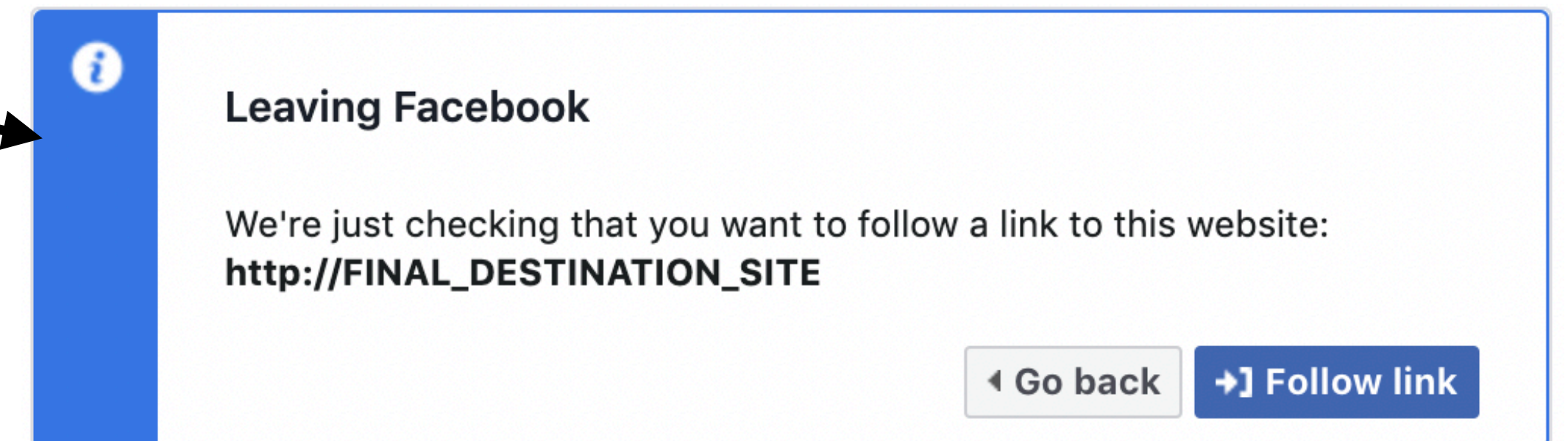
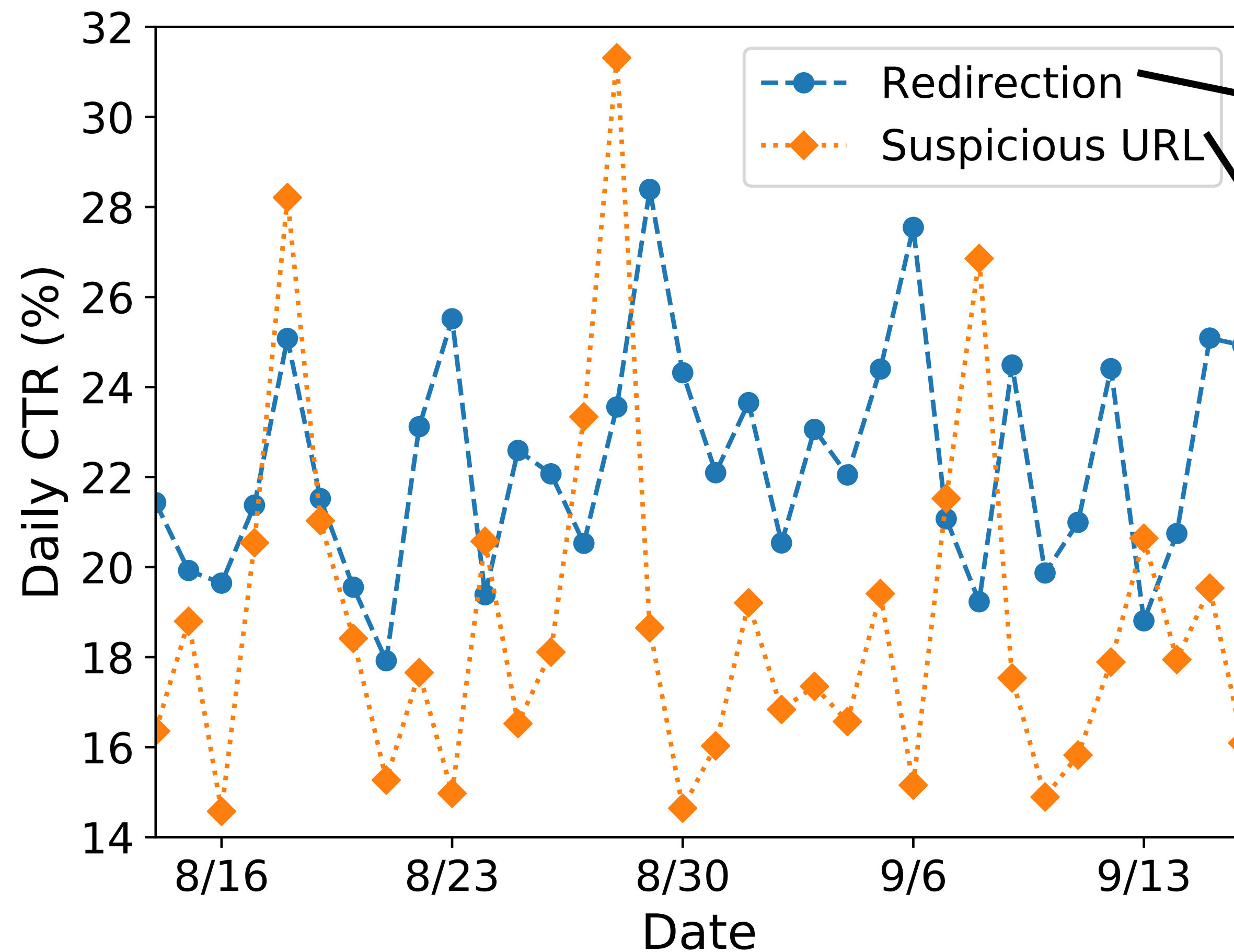
Navigation Source Privacy

Analyzed fraction of link shim browser clients within each class



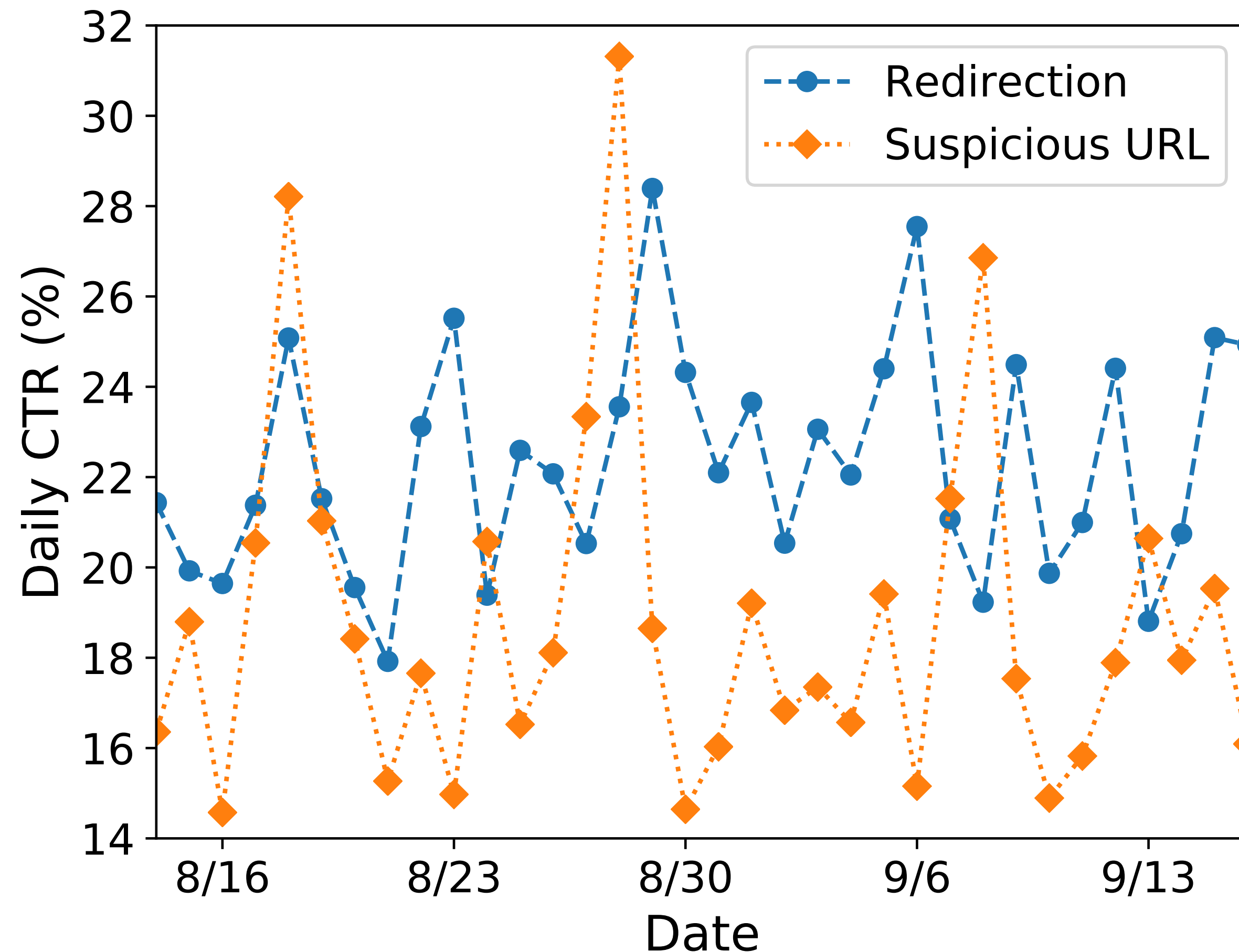
Navigation Destination Security

Analyzed warning clickthrough behavior



Navigation Destination Security

Analyzed warning clickthrough behavior



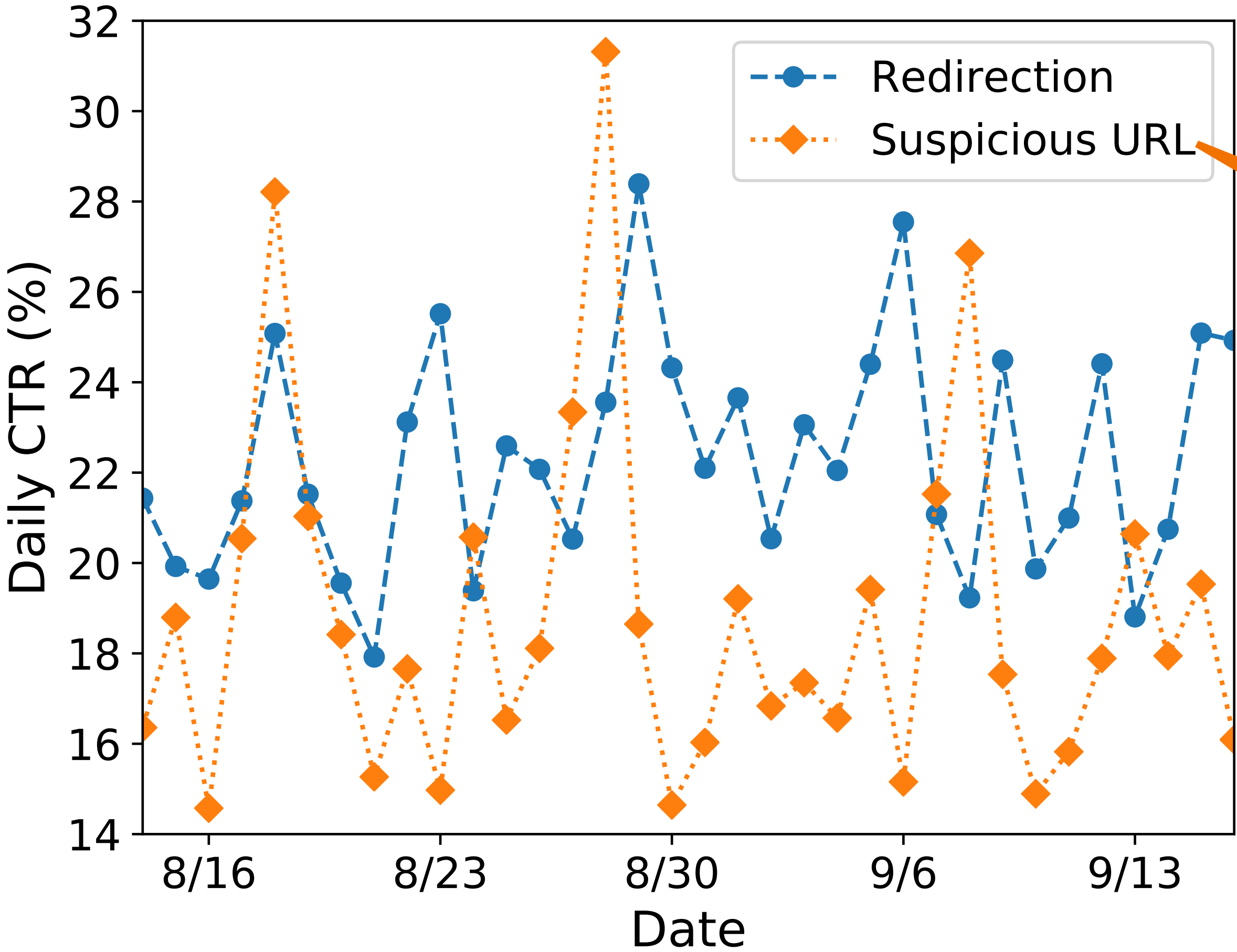
Browser warning
clickthrough rates ^[1]:

7.2 - 23.2%

[1] Devdatta Akhawe and Adrienne Porter Felt. "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness." USENIX Security 2013.

Navigation Destination Security

Analyzed warning clickthrough behavior

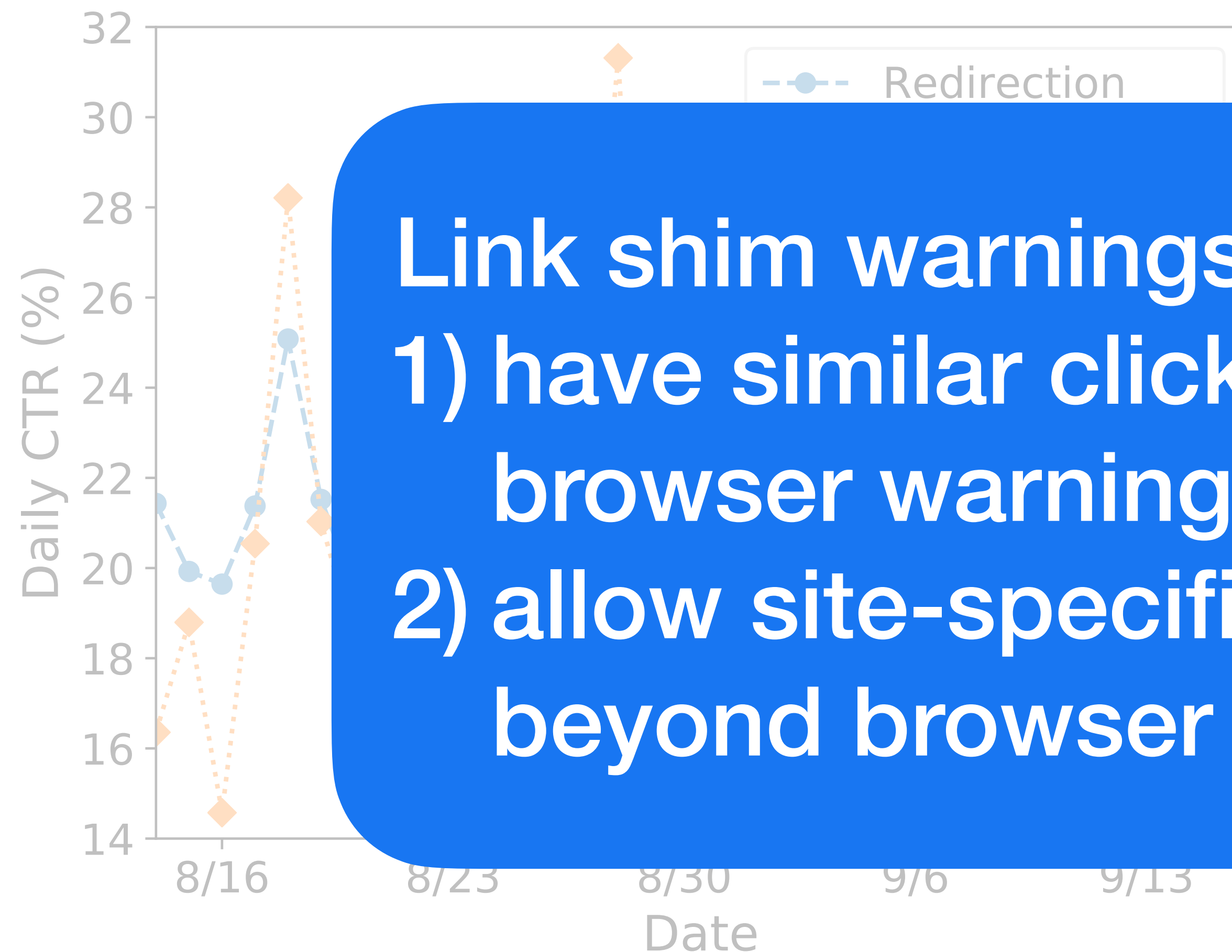


Only ~3% of URLs
appeared in Google
Safe Browsing

Adrienne Porter
and: A Large-Scale
Field Study of Browser Security Warning
Effectiveness." USENIX Security 2013.

Navigation Destination Security

Analyzed warning clickthrough behavior



Link shim warnings

1) have similar clickthrough rates to browser warnings

2) allow site-specific URL detection, beyond browser blocklists

warning rates [1]:

Adrienne Porter
nd: A Large-Scale
Security Warning
Security 2013.

More Results in the Paper!

- Impact of link shimming's navigation protocol upgrading
- Legacy browser populations for different OSes and countries
- Link shim warning adherence for different browsers, OSes, and countries.
- Adherence when re-encountering a warning
- Safety of user clickthrough decisions



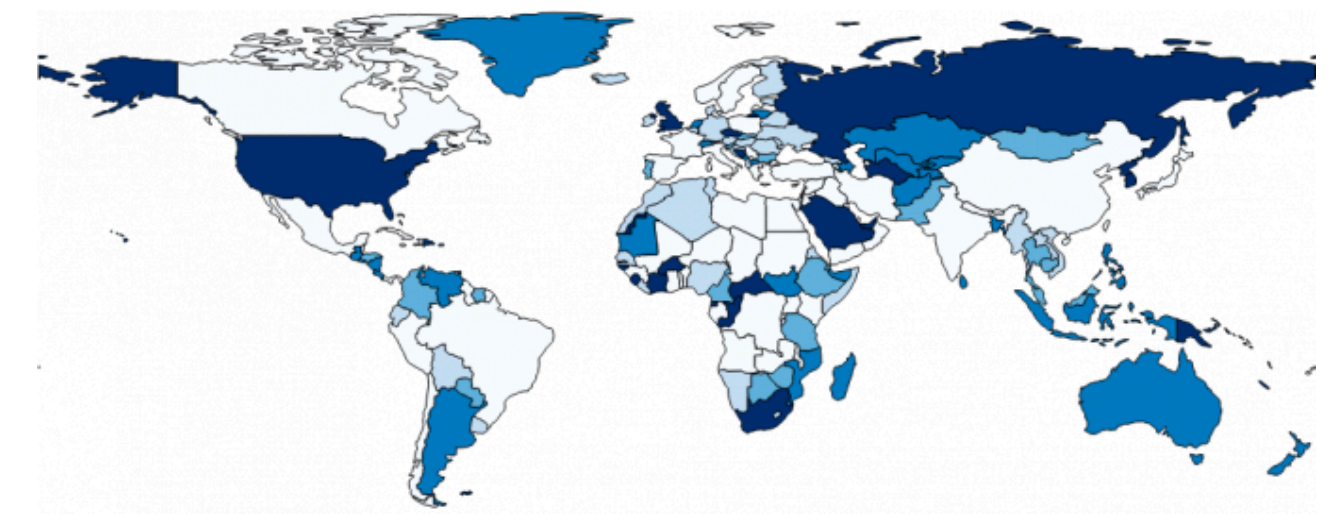
Lessons Learned

Despite modern browser features, link shimming can improve link navigation security & privacy.

(Costs: navigation performance, data collection)



Legacy scenarios are prevalent and important.



Website warnings can be effective.



Web security responsibilities are distributed.

Thanks!

frankli@gatech.edu

@frankli714