Melting Pot of Origins

Compromising the Intermediary Web Services that Rehost Websites

Takuya Watanabe[†‡], Eitaro Shioji[†],
Mitsuaki Akiyama[†], Tatsuya Mori[‡§⊥]

[†]NTT Secure Platform Laboratories,
[‡]Waseda University, [§]NICT, [⊥]RIKEN AIP

Panel in WAC 2021

This work...

- Presented at NDSS'20
- Study security flaws of *web rehosting services*
- Demonstrate five client-side attacks on real services
- Provide countermeasures

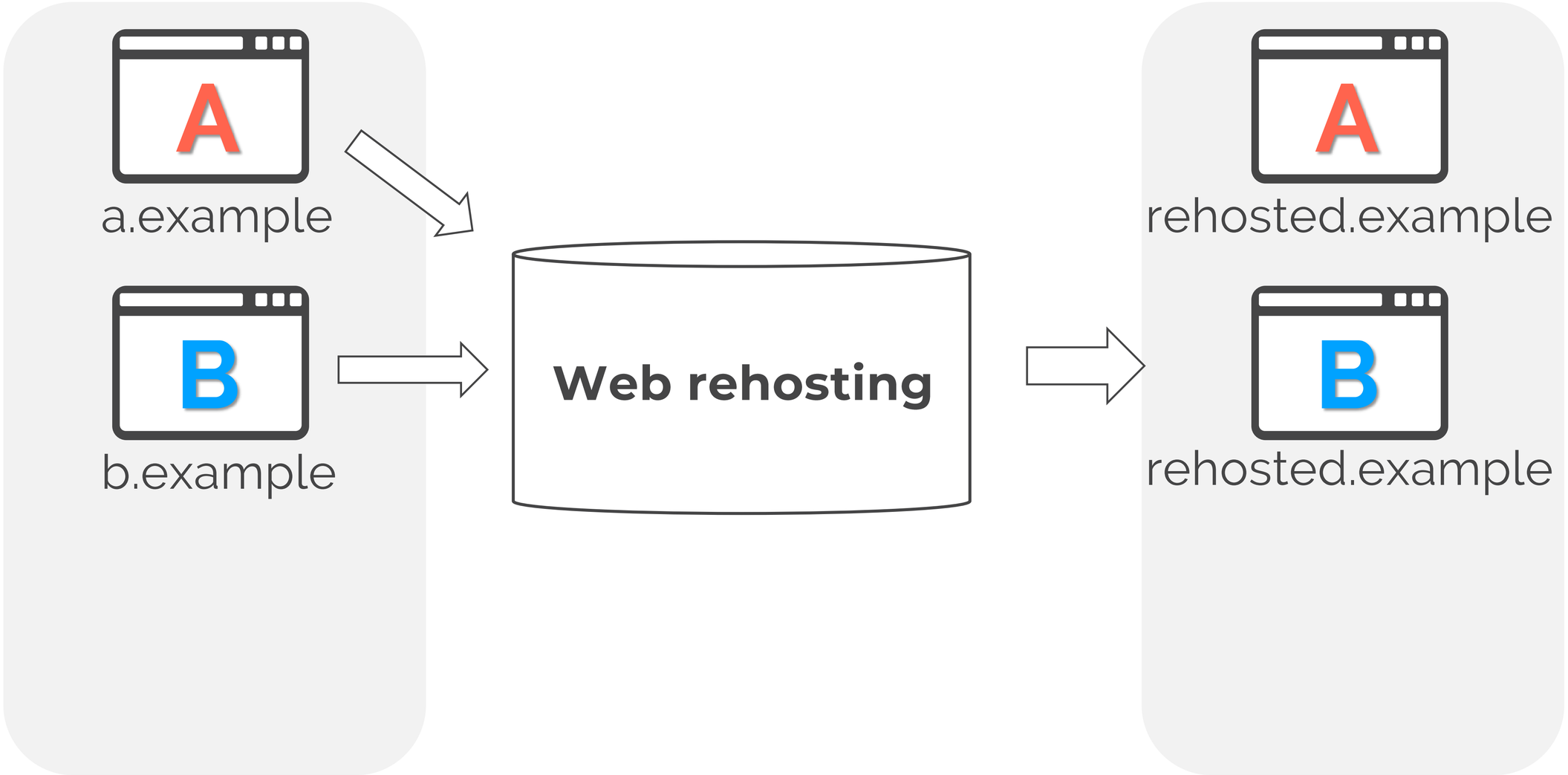
Web Rehosting Services Enhance Openness of Web

Website translator

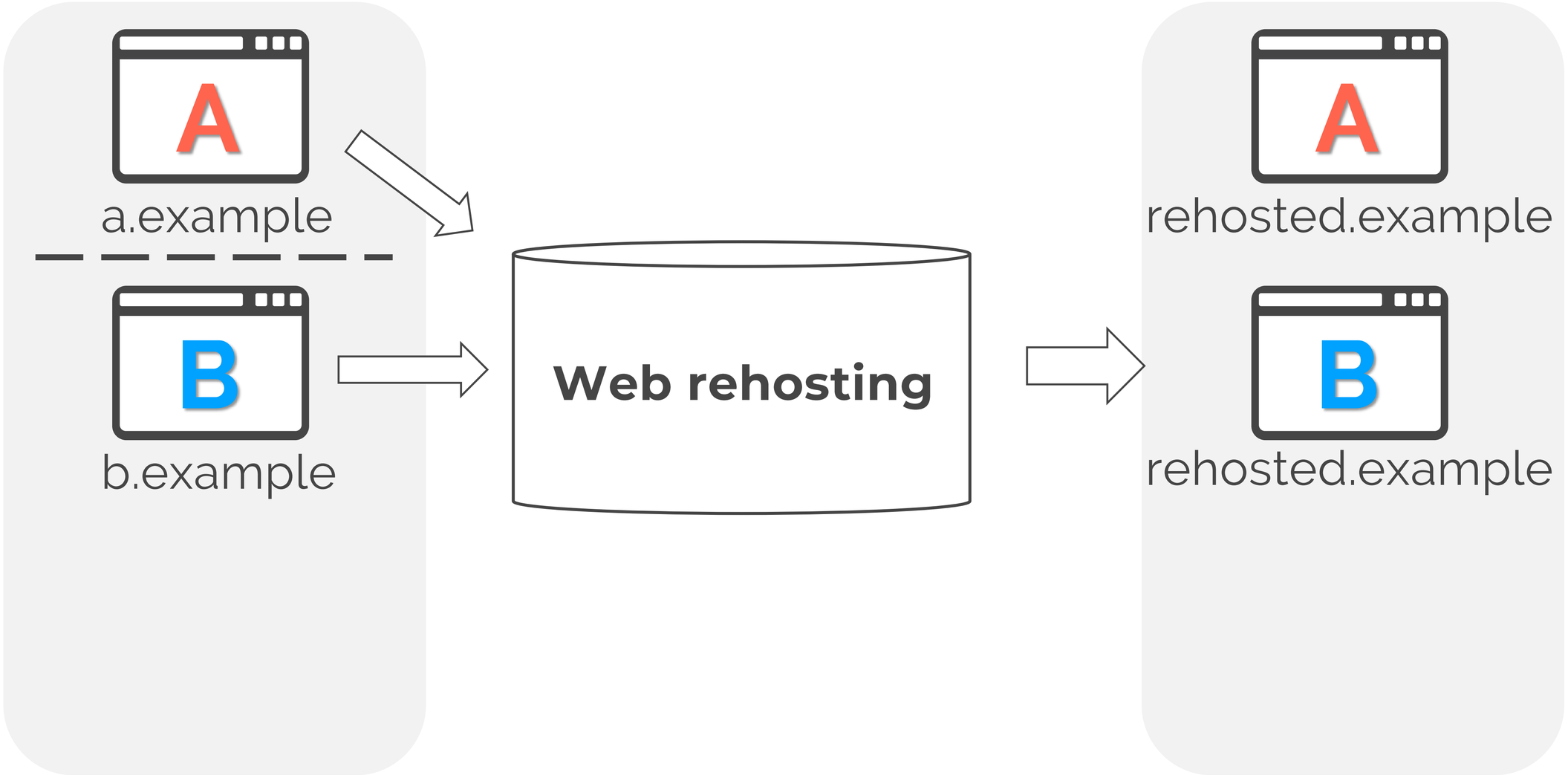
Web archive

Web-based proxy

Web Rehosting Architecture

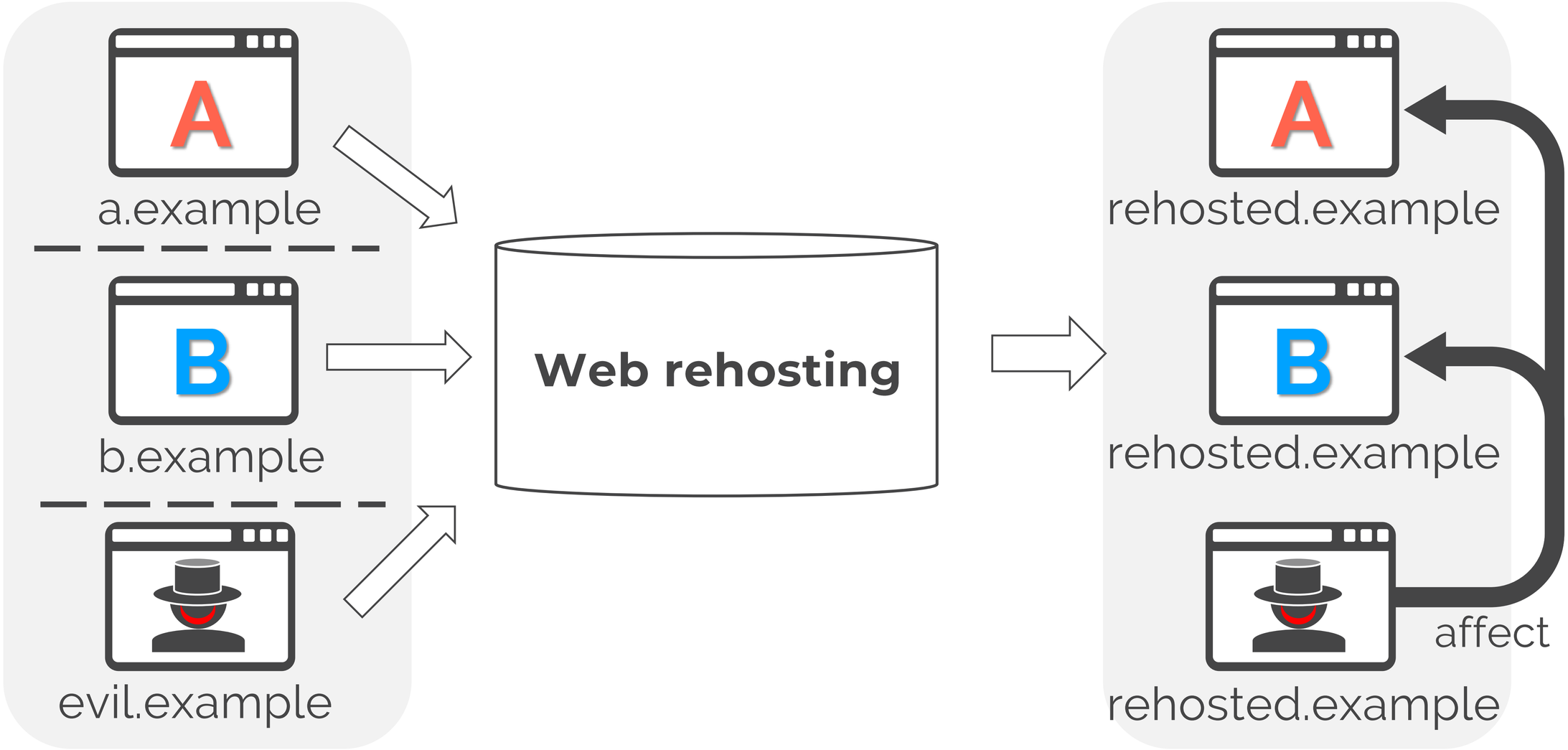


Web Rehosting Architecture



(— — — Boundary of origins)

Attack Surface



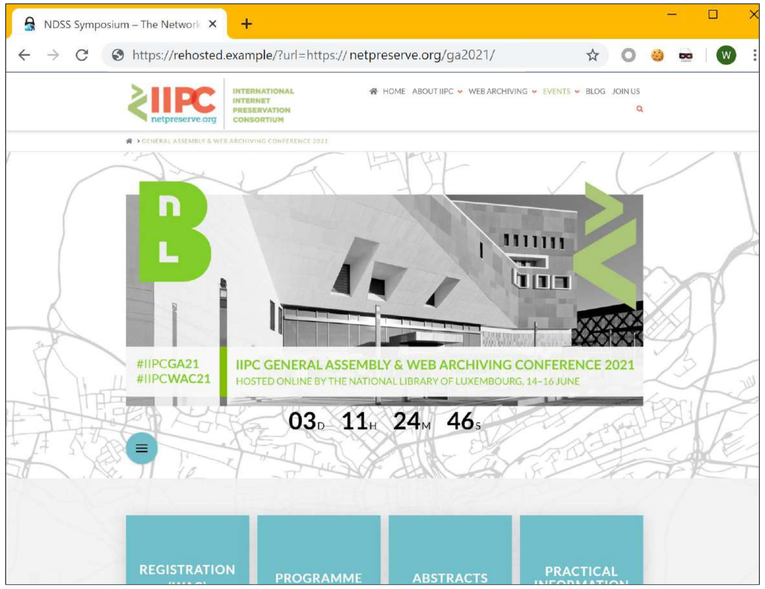
Attack Surface

Attacks against Web Rehosting

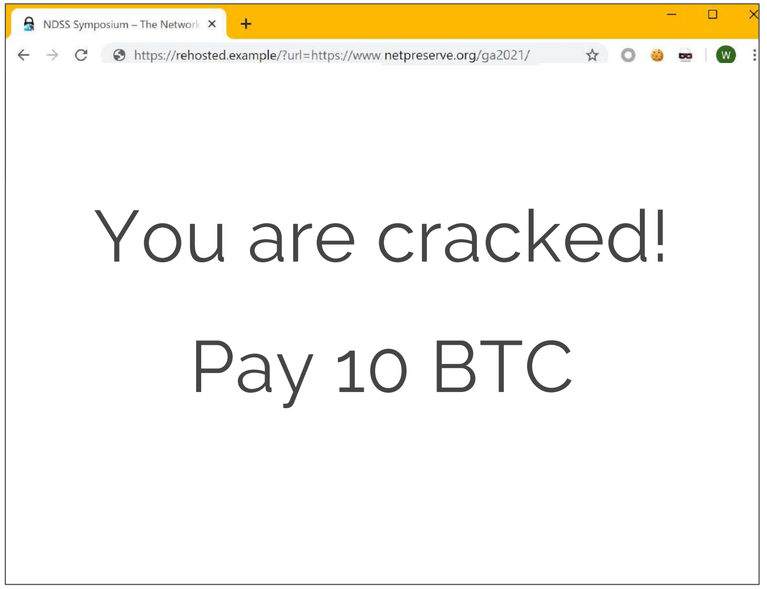
#	Attacks	Exploited Resources	Work on Web Archive?
I	Persistent MITM	Service Worker, AppCache	✔
II	Privilege Abuse	Camera, Microphone, Location, etc.	✔
III	Credential Theft	Password Manager	
IV	History Theft	Cookie, localStorage	✔
V	Session Hijacking	Cookie	

Attack I: Persistent MITM

Direct



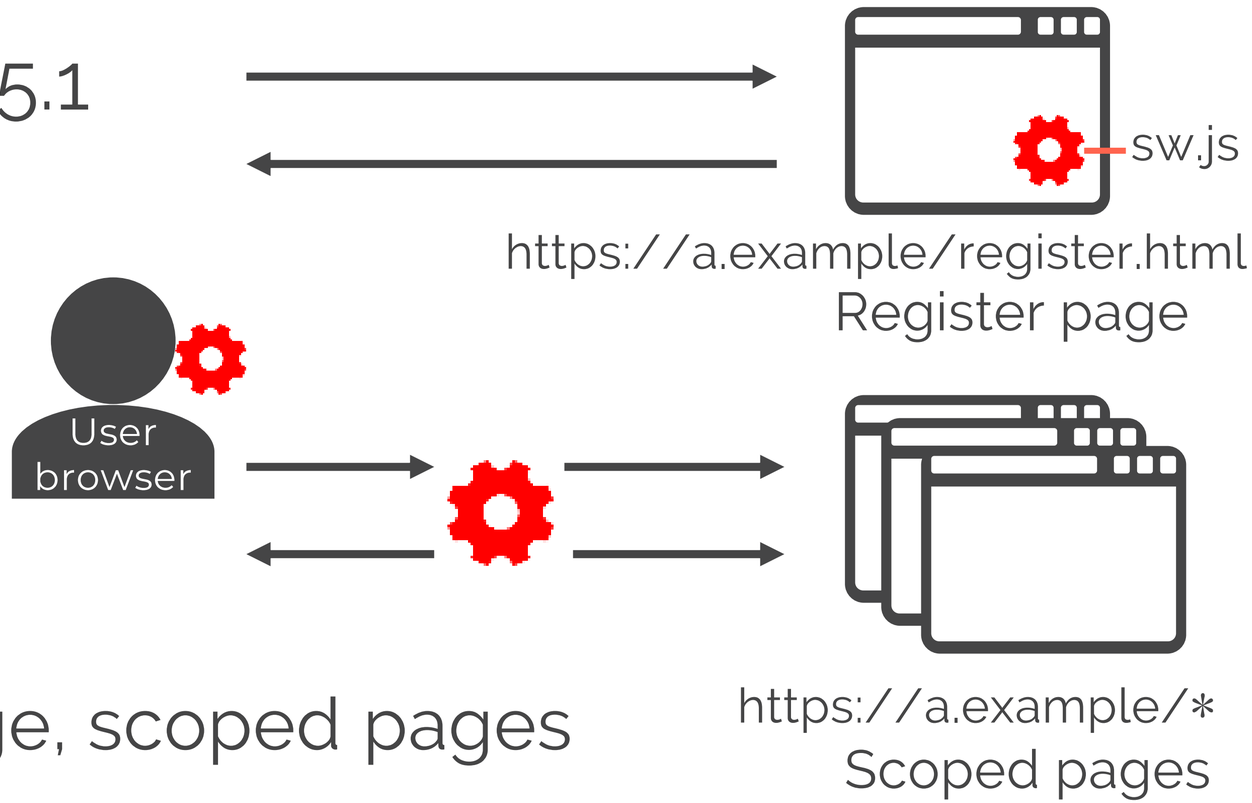
Through web rehosting



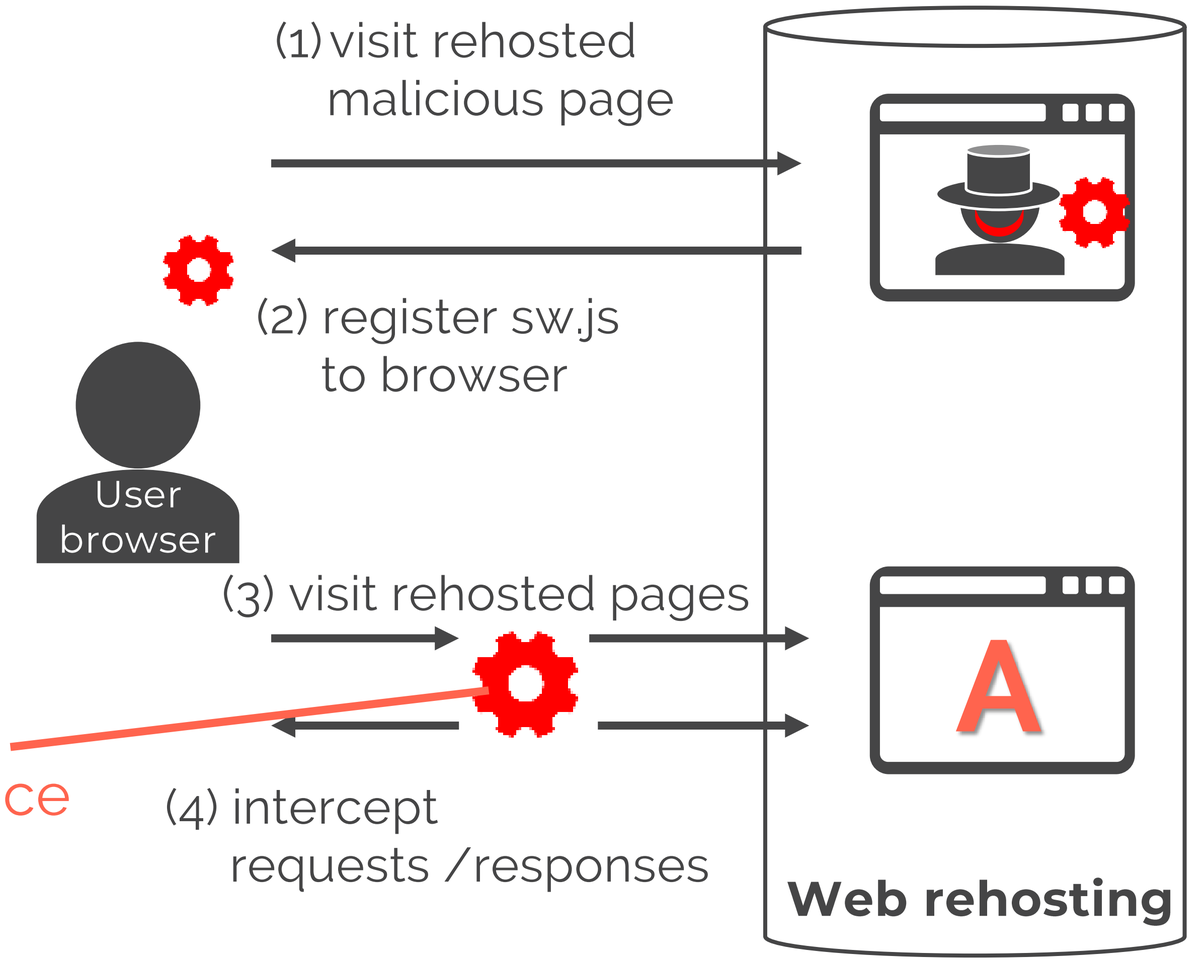
Through web rehosting (after attack)

Service Worker (SW)

- Powerful feature in HTML 5.1
  - intercept all req./res.
- Restrictions
  - HTTPS
  - Same Origin
    - SW script, register page, scoped pages
  - MIME Type (JavaScript)

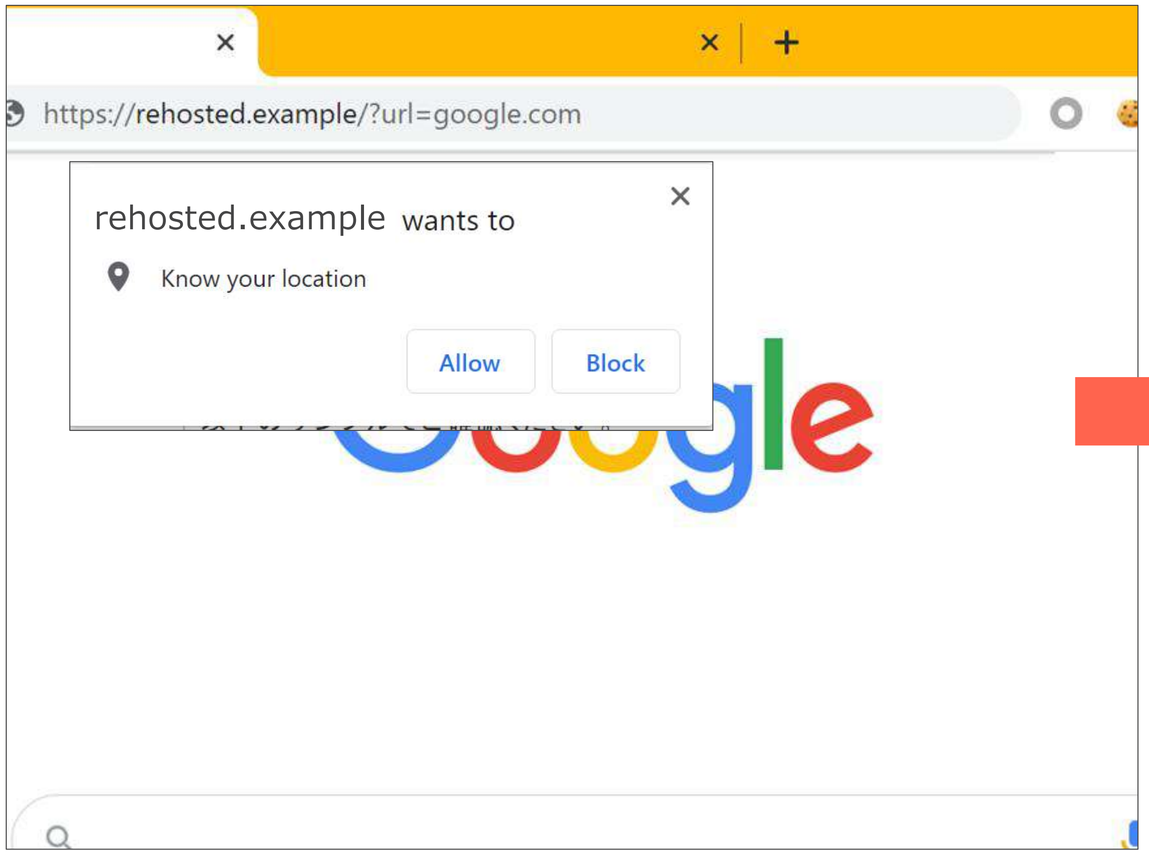


Attack I: Persistent MITM (with SW)

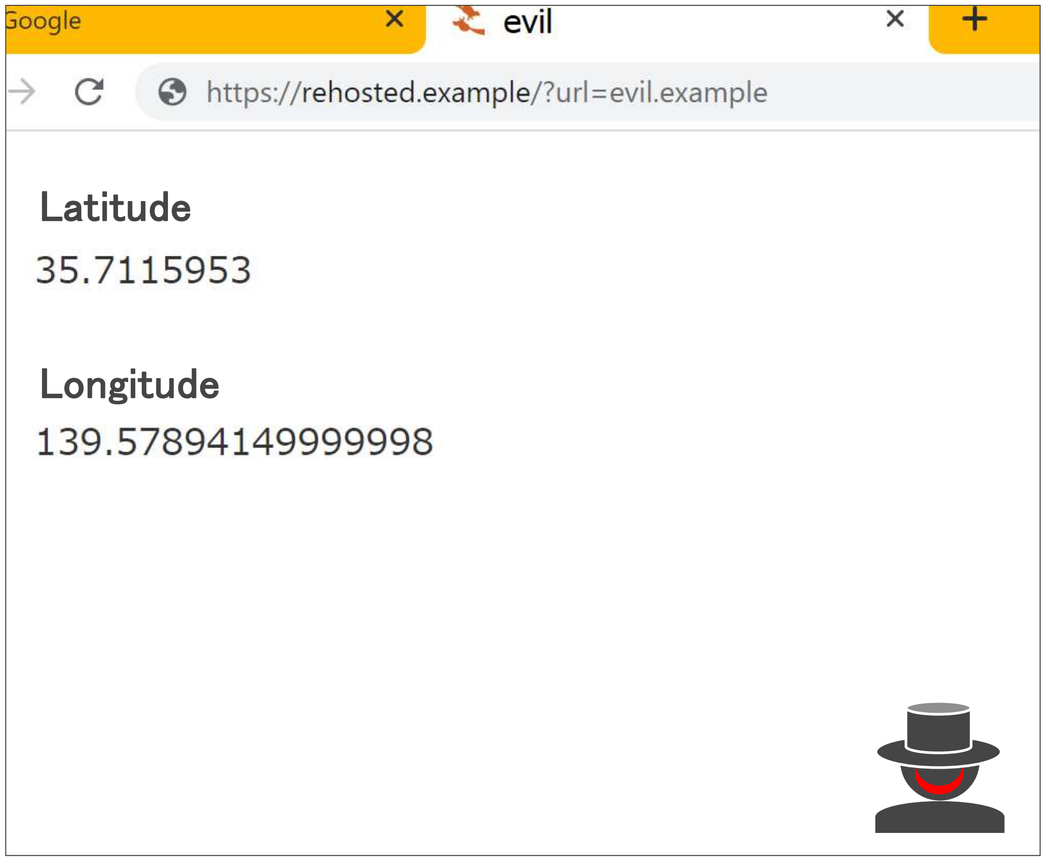


Scope: origin of
web rehosting service

Attack II: Privilege Abuse



User grant permission
at rehosted benign pages



Permission is reused by
rehosted **malicious** page

Attack IV: History Theft

1. User visits rehosted page.
2. Page writes cookie or localStorage by using JavaScript.

```
document.cookie = "unique=string";
```

3. Rehosted malicious page retrieves cookie/localStorage.
4. Attacker estimates browsing history by using retrieved data.

Summary of Results

● Vulnerable

○ Secure

Category	Rehosting Service	Scheme	At least one Vulnerability	Persistent MITM		Privilege Abuse	Credential Theft	History Theft	Session Hijacking & Injection
				SW	AppCache				
Proxy	ProxySite	HTTPS	●	●	●	●	●	●	●
	Hide My Ass!	HTTPS	●	●	●	●	●	●	○
	Hide me	HTTPS	●	●	●	●	●	●	●
	Sitenable Web Proxy	HTTPS	●	●	●	●	●	●	●
	FilterBypass	HTTPS	○	○	○	○	○	○	○
	ProxFree	HTTPS	●	●	●	●	●	●	●
	toolur	HTTPS	●	●	●	●	●	●	●
	hidester	HTTPS	●	●	●	●	●	●	●
	GenMirror	HTTPS	○	○	○	○	○	○	○
	UnblockVideos	HTTPS	●	●	●	●	●	●	●
	Service-α	HTTP/S	●	●	●	●	●	●	●
Translator	Google Translate	HTTPS	●	●	○	○	—	●	—
	Bing Translator	HTTPS	●	○	○	○	—	●	—
	Weblio	HTTPS	●	○	○	●	—	●	—
	PROMT Online	HTTP	●	○	○	○	—	●	—
	Service-β	HTTPS	●	●	○	●	—	●	—
	Yandex.Translate	HTTPS	●	●	●	○	—	●	—
	Baidu Translate	HTTP	●	○	○	○	—	●	—
Archive	Wayback Machine	HTTPS	●	●	●	●	—	●	—
	Google Cache	HTTP/S	●	○	○	●	—	●	—
	FreezePage	HTTP	○	○	○	○	—	○	—

Trust in Web Archives from Client-Side Security Perspective

- Threats from different directions
  - falsifications and privacy violations
- Evolution of web features vs. web archives architecture
  - HTML5, CORS, Progressive Web
- Difficulty in observing attack damage
  - Who is a real victim?

watanabe@nsl.cs.waseda.ac.jp @twatanabe1203