PPSB: An Open and Flexible Platform for Privacy-Preserving Safe Browsing

Helei Cui[1], Yajin Zhou[2], Cong Wang[1], Xinyu Wang[1], Yuefeng Du[1], Qian Wang[3]
[1]City University of Hong Kong, [2]Zhejiang University, [3]Wuhan University

Open source code: https://github.com/ppsb201804/PPSB

1. Background

Fig. 1: *Safe Browsing services, e.g., Google Safe Browsing (GSB), keep users from unsafe websites that can harm their devices with malware or phishing content.*

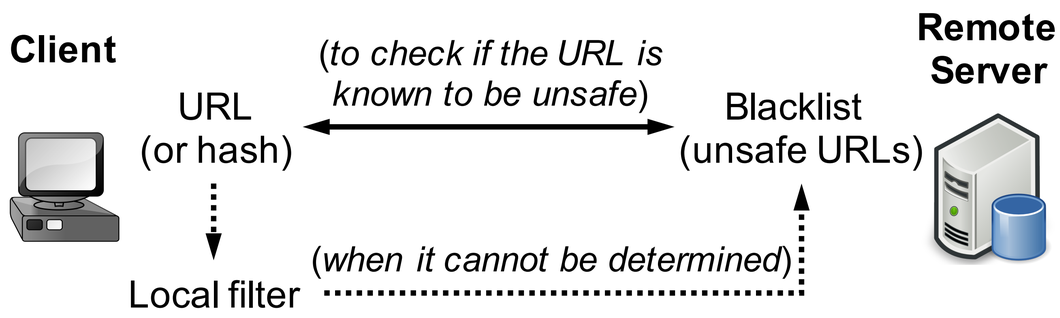

Fig. 2: *General procedure of Safe Browsing (SB) services.*

2. Problem

To detect unsafe URLs, existing SB services require the sharing of visited URLs, either in cleartext, full-length hash, or 4-32 bytes hash prefix.

- URLs or full-length hashes could be used for **tracking** users;
- Even the hash prefixes (used in GSB) could be abused for **inferring** users' browsing history:
  - The number of URLs/domains on the web is **finite**;
  - Using **multiple matched prefixes** can narrow down the candidates for URL/domain inference.

This undoubtedly violates the user privacy and should be fixed ASAP due to its extremely large user base.

Table 1: *Summary of **data collected** by popular SB services.*

SB Service	Data Collected	Known Products
GSB (Update API)	Hash prefix(es) of URL	Chrome, Safari, Firefox, Android WebView, etc.
GSB (Lookup API)	Full URL	-
Windows Defender SmartScreen	Full URL	Windows, IE, Edge, and Chrome Extension
Opera Fraud and Malware Protection	Domain & hash of URL	Opera

3. Our Solution

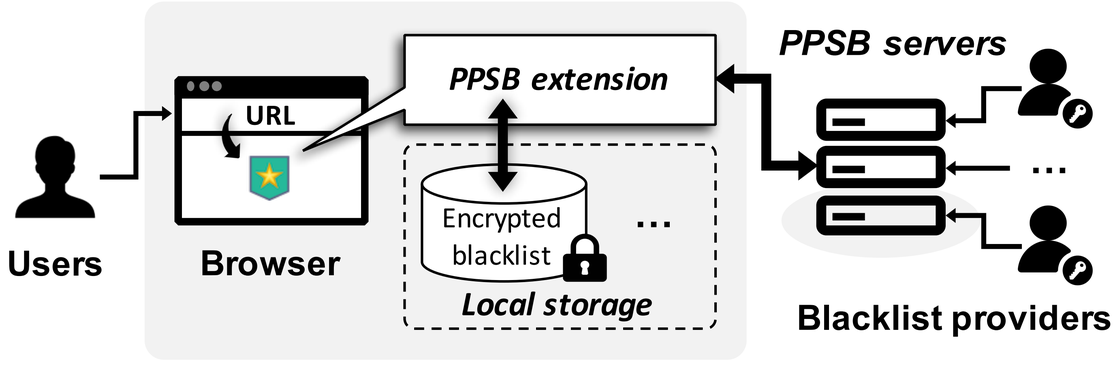

Fig. 3: *Overview of our proposed PPSB service.*

In PPSB, the URLs to be checked (or vetted) are never leaked to service provider (or extra blacklist providers), while the list of unsafe URLs are protected and not easily be revealed by client applications.

- Privacy-preserving and fast processing
- Backward compatible and easy customization
- Fast deployment and auto synchronization

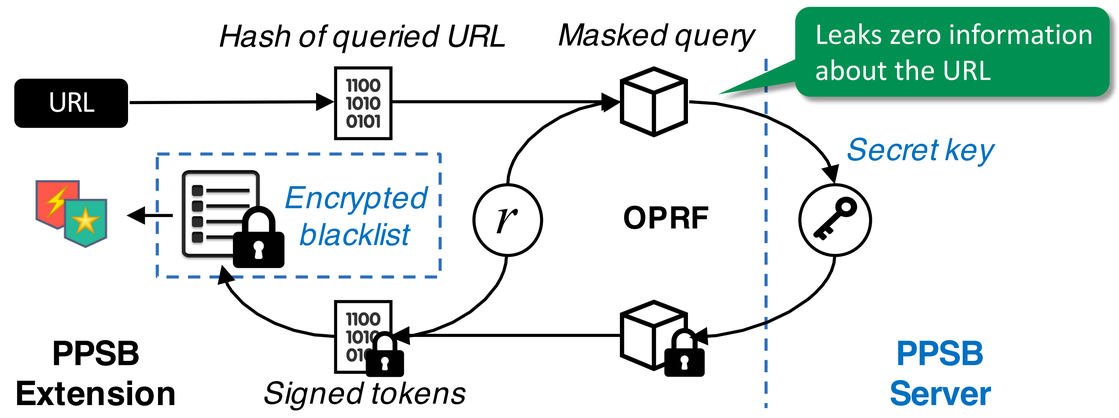

Fig. 4: *The query flow of encrypted matching when there is a match in the local prefix filter.*

4. Prototype Evaluations

- Three real blacklists: #1 - ***PhishTank*** (36,473 verified unsafe URLs), #2 - ***MalwareDomains*** (20,956 malware domains), and #3 - ***Shallalist*** (over 1.7 M unsafe domains and URLs).

Table 2: *Average load time of unsafe URLs - PPSB operates **at the millisecond level** while protecting the privacy.*

Platform	GSB (ms)	MSB (ms)	PPSB w/ #1 (ms)	PPSB w/ #1,2 (ms)	PPSB w/ #1,2,3 (ms)
Windows	112	116	333	388	437
macOS	184	194	340	373	440
Ubuntu	67	155	329	354	431

**MSB - Windows Defender Browser Protection, which is a recently released Chrome extension by Microsoft.*

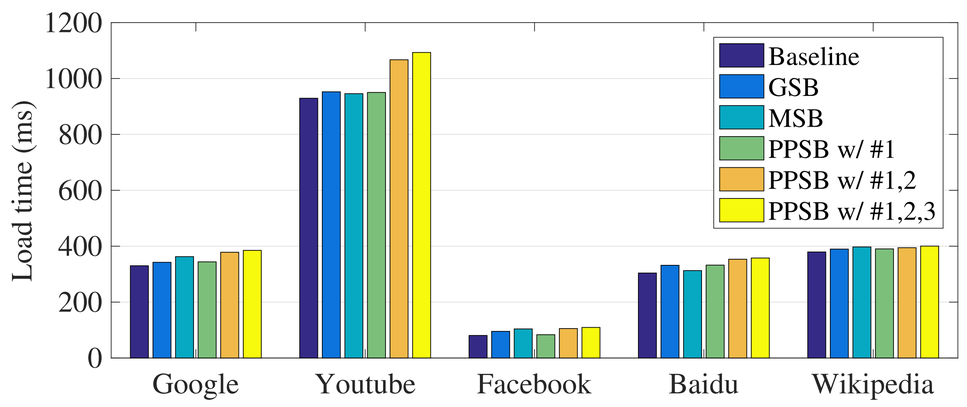

Fig. 5: *Average load time of five famous (safe) websites - PPSB achieves the same user experience as others.*

5. Concluding Remarks

PPSB: safe browsing with **the guaranteed privacy** of users and blacklist providers (who can easily set up its own server).

Watch demo on YouTube

Install **PPSB** on Chrome Web Store

Contact: Helei Cui (cuihelei@outlook.com), Yajin Zhou (yajin_zhou@zju.edu.cn), and Cong Wang (congwang@cityu.edu.hk). Acknowledgment: This work was supported by the RGC of Hong Kong (Project No. C1008-16G, and CityU 11276816), and the NSFC (Project No. 61572412).