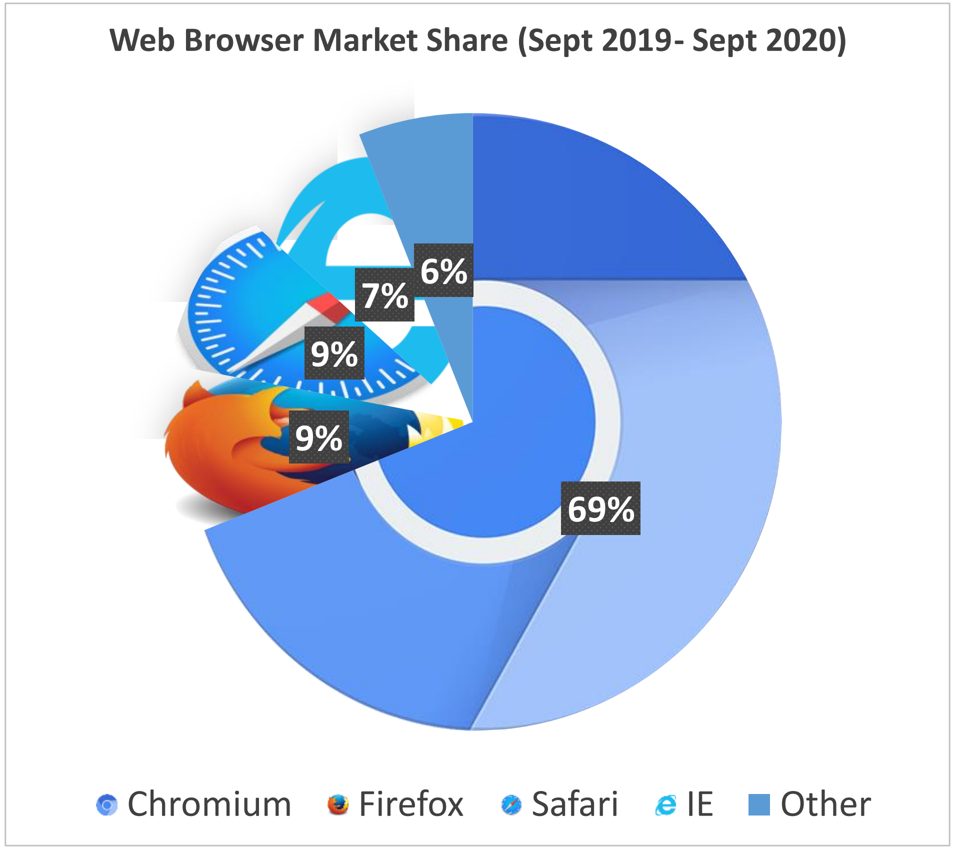
Slimium: Debloating the Chromium Browser with Feature Subsetting

CHENXIONG QIAN, HYUNGJOON (KEVIN) KOO,
CHANGSEOK OH, TAESOO KIM, WENKE LEE

Background

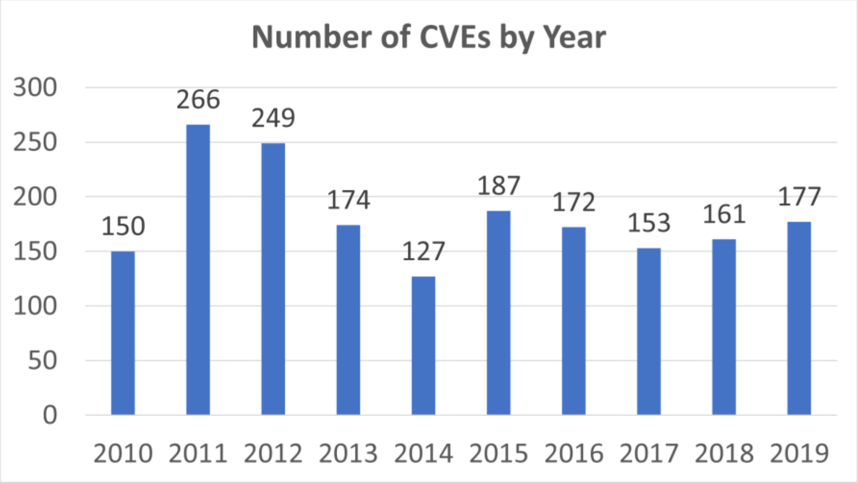
- Chromium dominates Web browser market share.

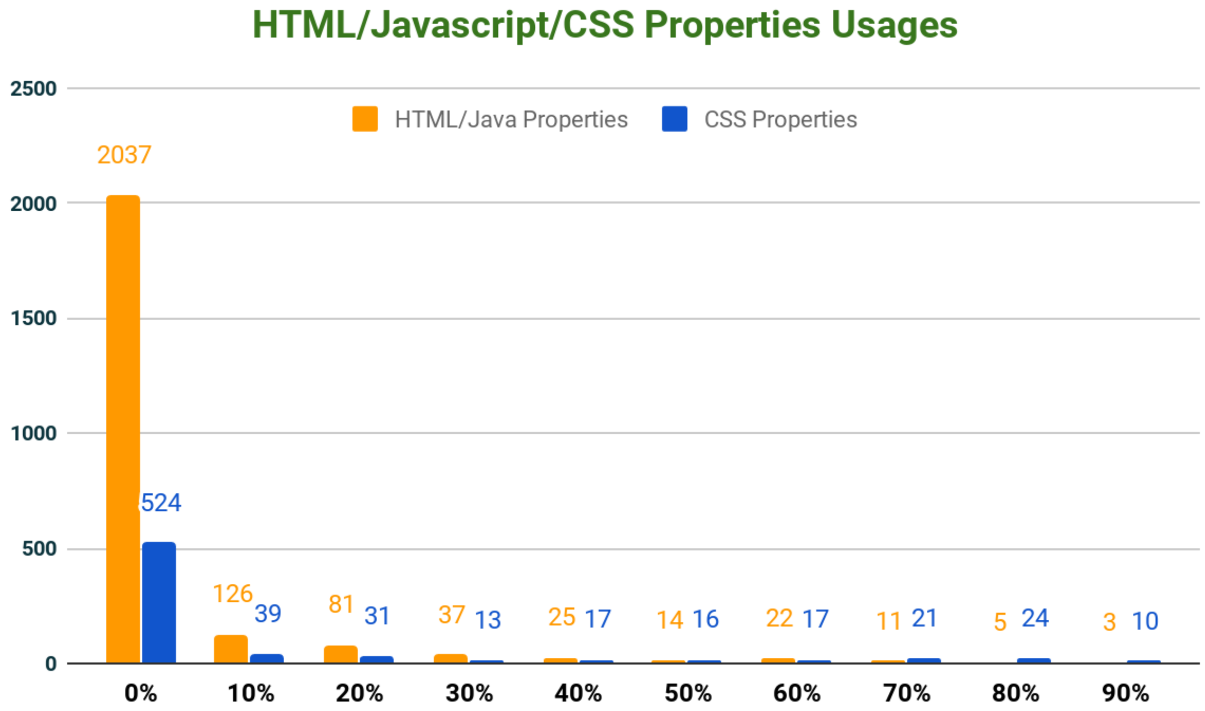
- Ever-increasing Features:
  - 2300+ Html/Javascript properties
  - 700+ CSS properties
  - Hundreds of experimental features



Problem

- Not all features are used commonly.
- Attack surface is increasing.





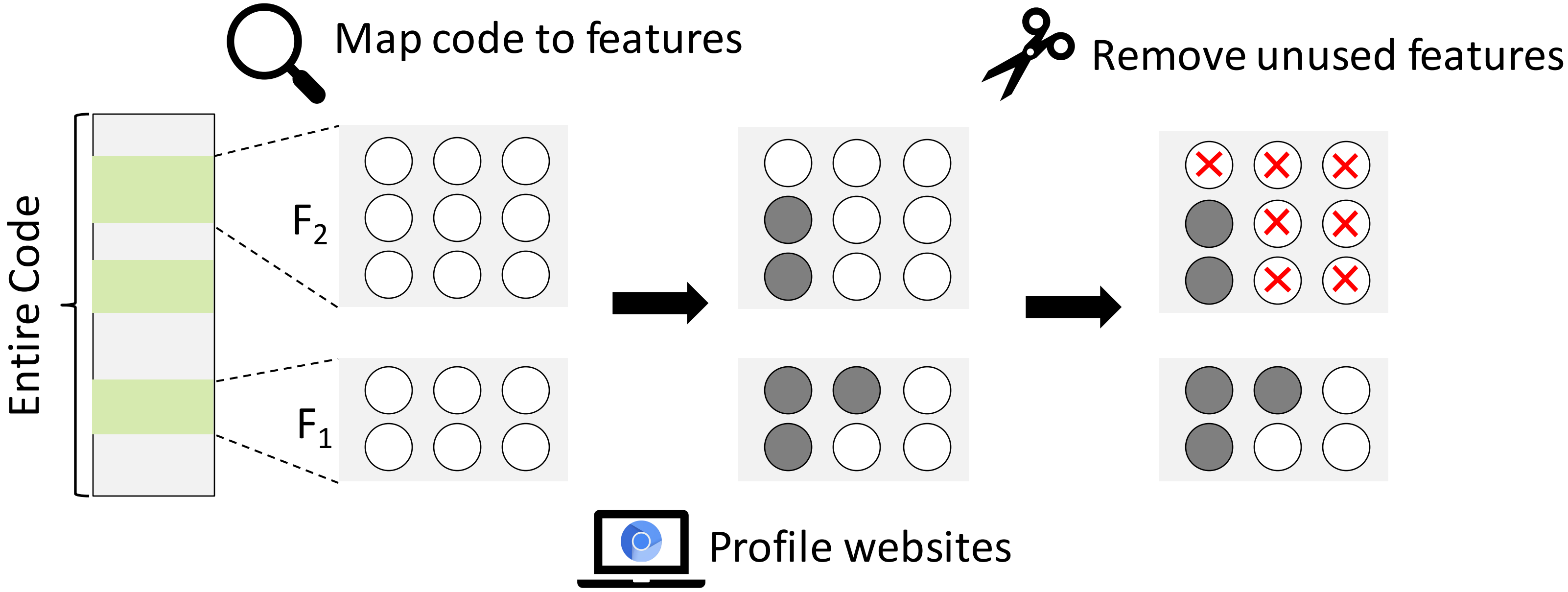
Feature Policy

Slimium

Remove code of unused features.

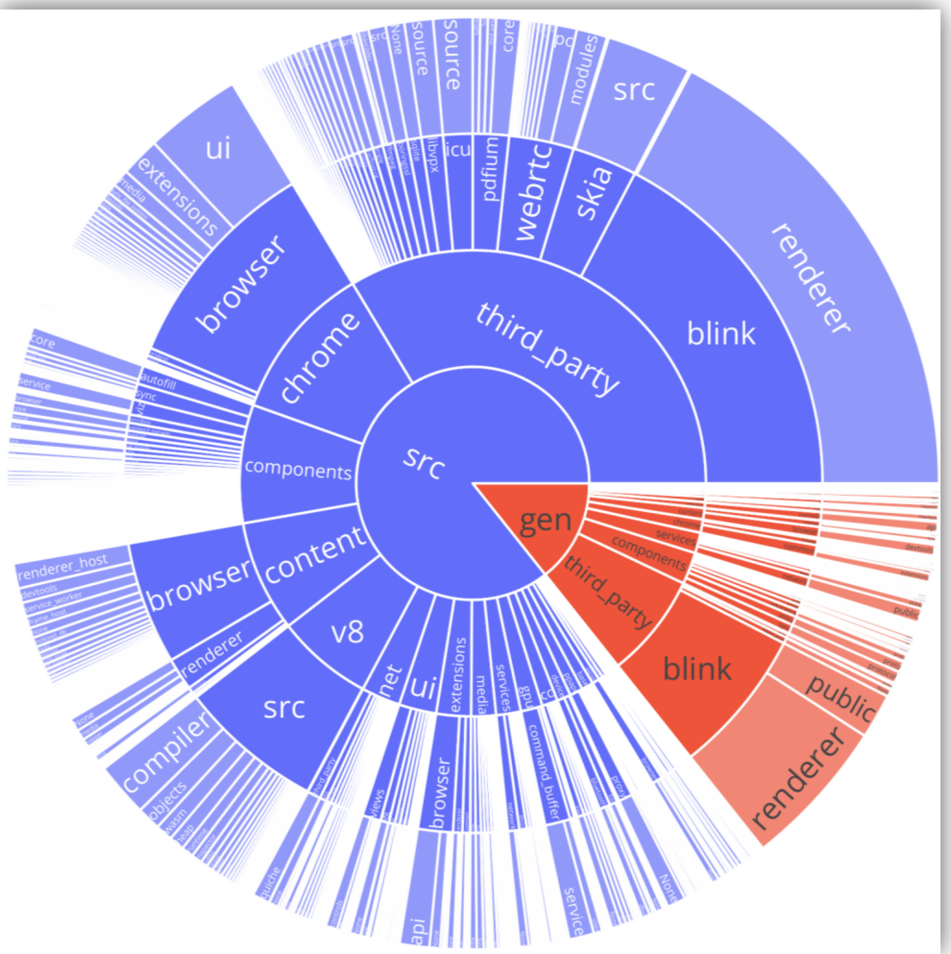
Given a set of websites, generate a slim version of Chromium.

Overview


Map code to features
Remove unused features
Entire Code
F2
F1
Profile websites

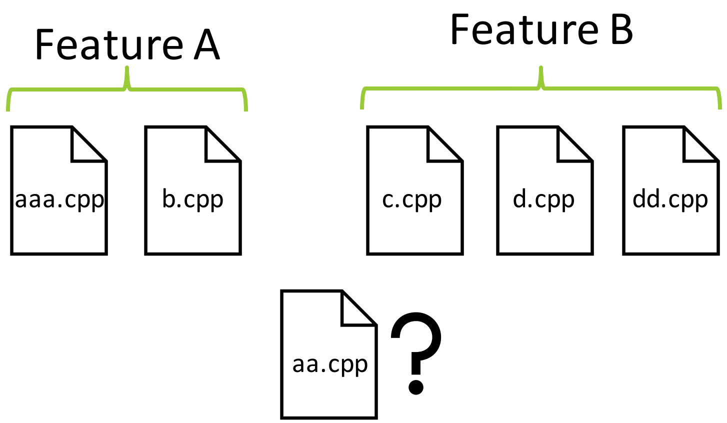
Feature Code Mapping

- Challenge
  - Large-scale & Complex
  - Code generation during compiling



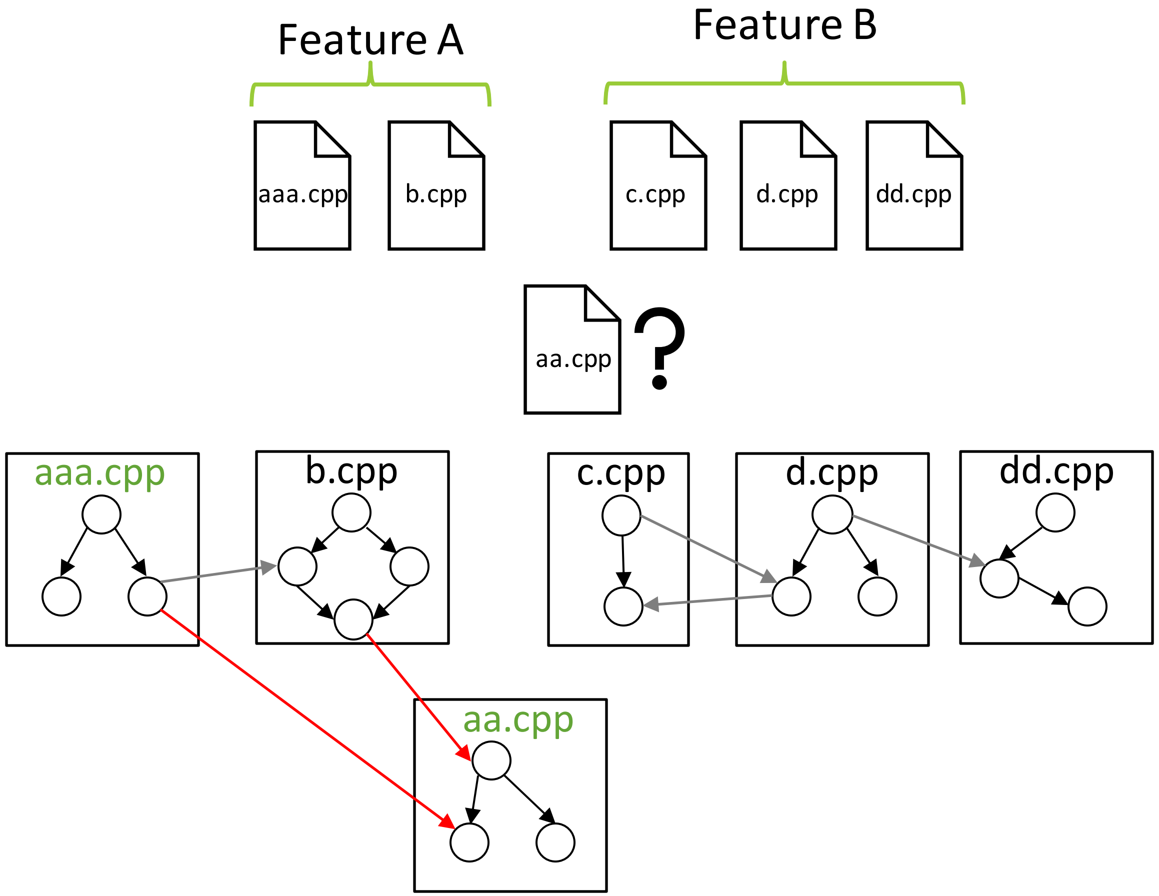
Feature Code Mapping

- Approach
  - Manual Analysis
    - Investigate source code and documents.
    - Create an initial mapping between features and source code (i.e., files).



Feature Code Mapping

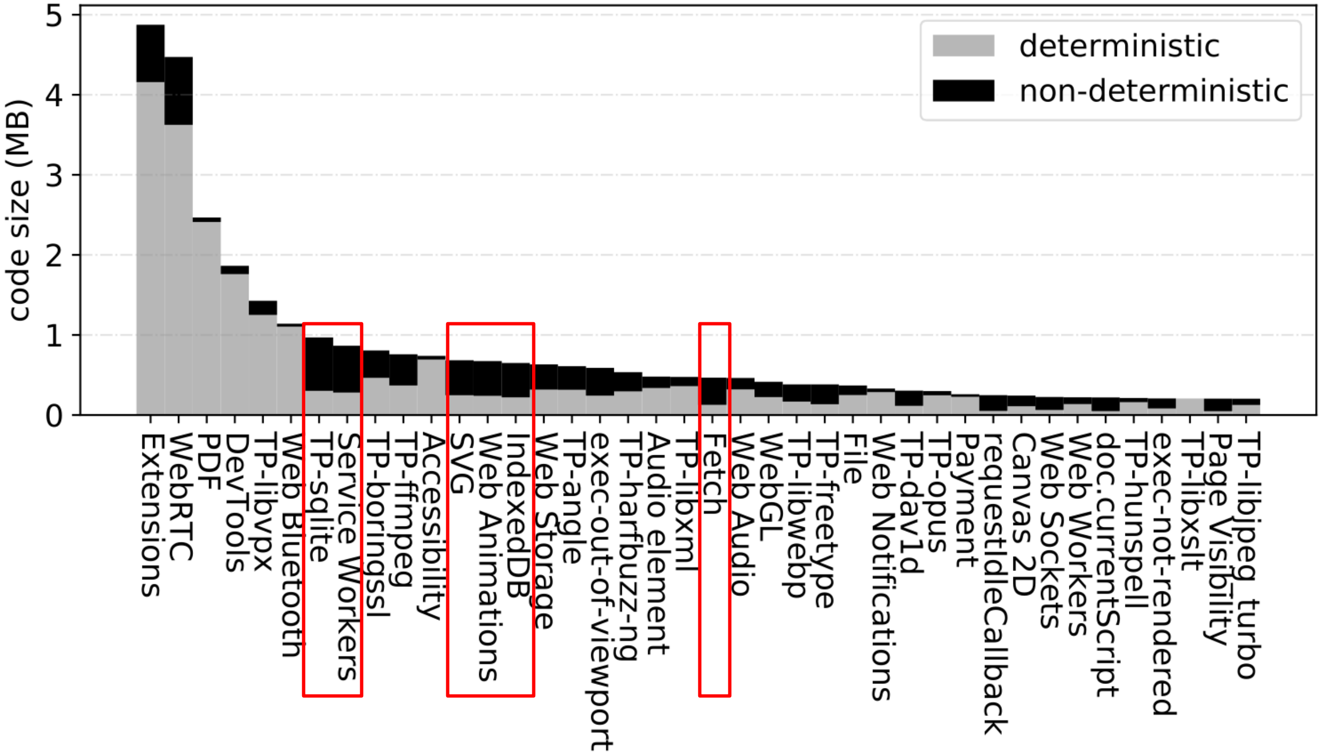
- Approach
  - Manual Analysis
    - Investigate source code and documents.
    - Create an initial mapping between features and source code (i.e., files).
  - Static Analysis
    - Build the call graph
    - Compute a relation vector $\boldsymbol{R} = (\boldsymbol{r_c}, \boldsymbol{r_s})$
      - $\boldsymbol{r_c}$ -- Call Invocation Relation (0 ~ 1)
      - $\boldsymbol{r_s}$ -- File Name Similarity (0 ~ 1)
    - If $\boldsymbol{r_c}$ and $\boldsymbol{r_s}$ are greater than the thresholds, add the file to the feature's mapping.



Webpage Profiling

- Challenge & Approach
  - Nondeterministic Code
    - Keep profiling until stable.
  - Performance
    - Adopt AFL’s approach.

Identified nondeterministic code from visiting the top 1000 Alexa websites

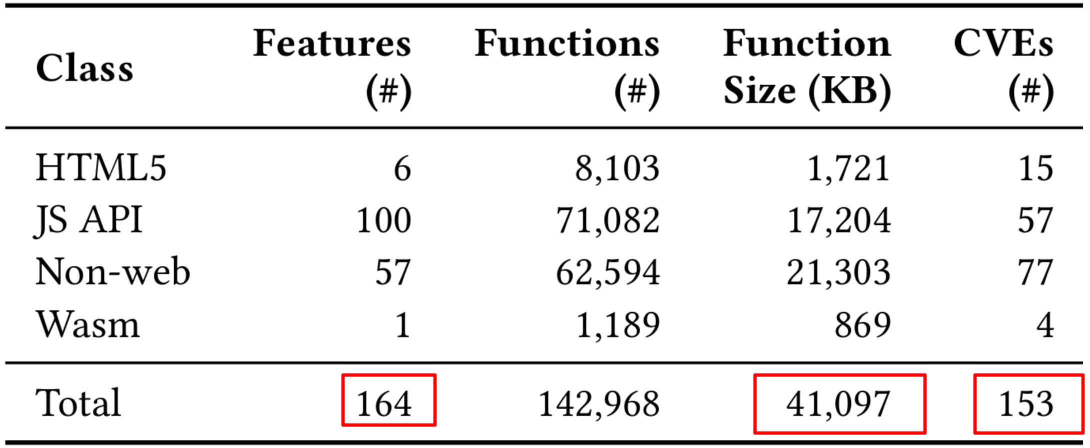


Removing Unused Features

- Keep nondeterministic code.
- Calculate a feature’s code coverage based on profiling results.
  - If the code coverage is greater than the threshold (i.e., $\boldsymbol{T}$), keep the feature.
  - Otherwise, remove the feature’s unexecuted code.
- Rewrite the binary to remove code.

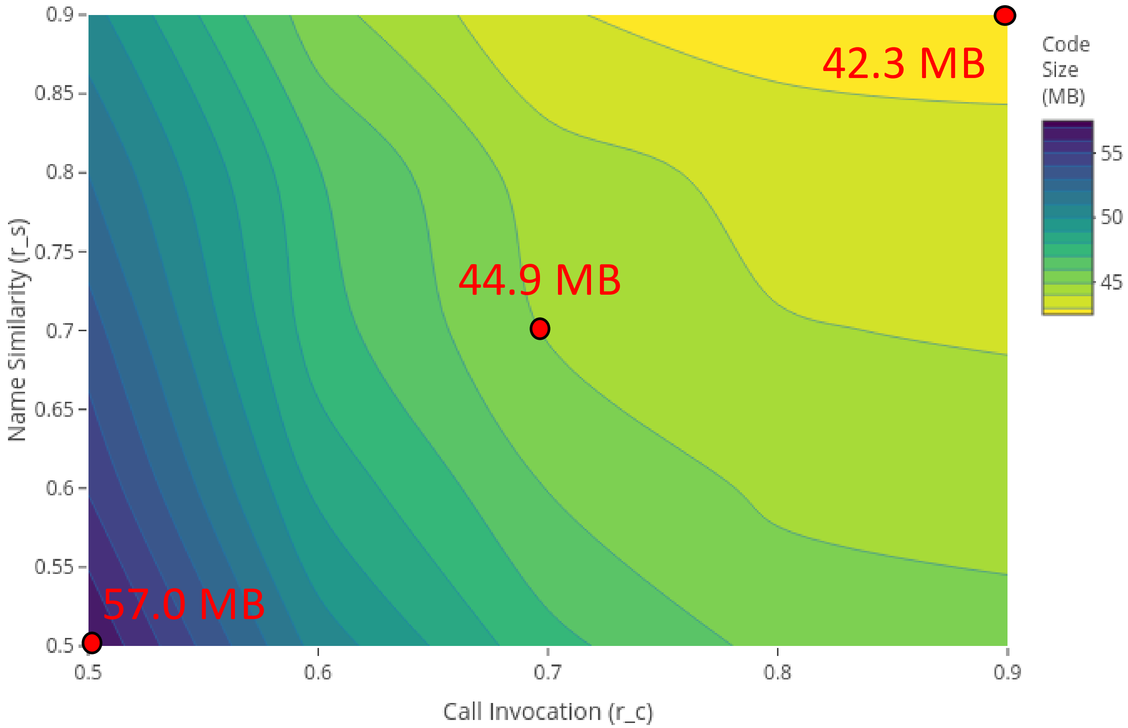
Evaluation

- Feature Code Mapping



Class	Features (#)	Functions (#)	Function Size (KB)	CVEs (#)
HTML5	6	8,103	1,721	15
JS API	100	71,082	17,204	57
Non-web	57	62,594	21,303	77
Wasm	1	1,189	869	4
Total	164	142,968	41,097	153

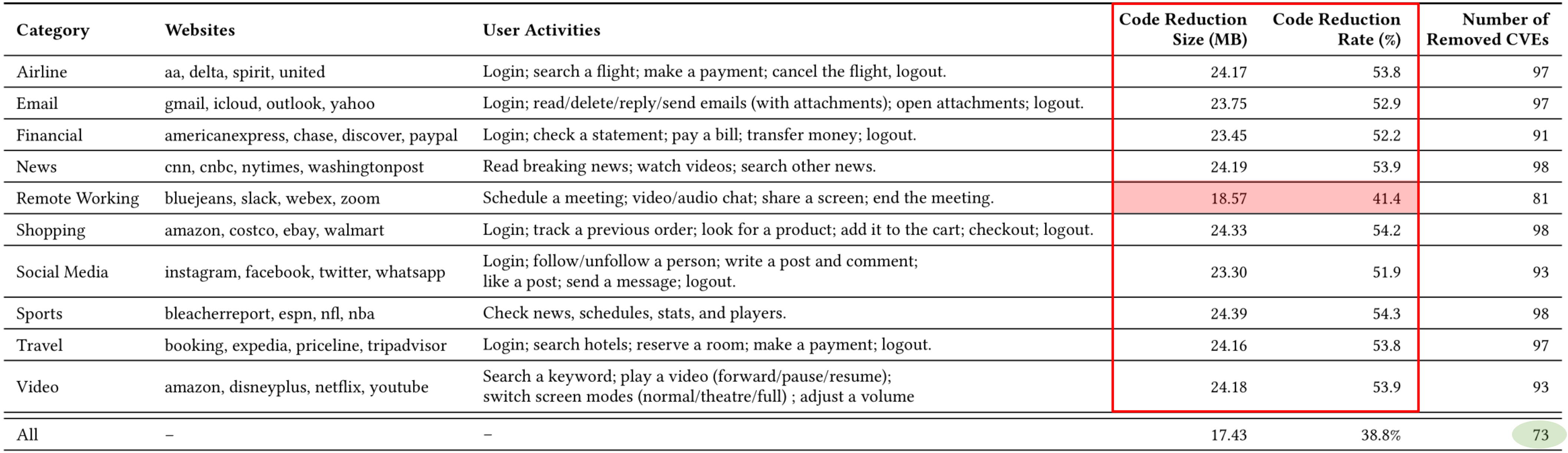
Manual Analysis



Static Analysis

Evaluation

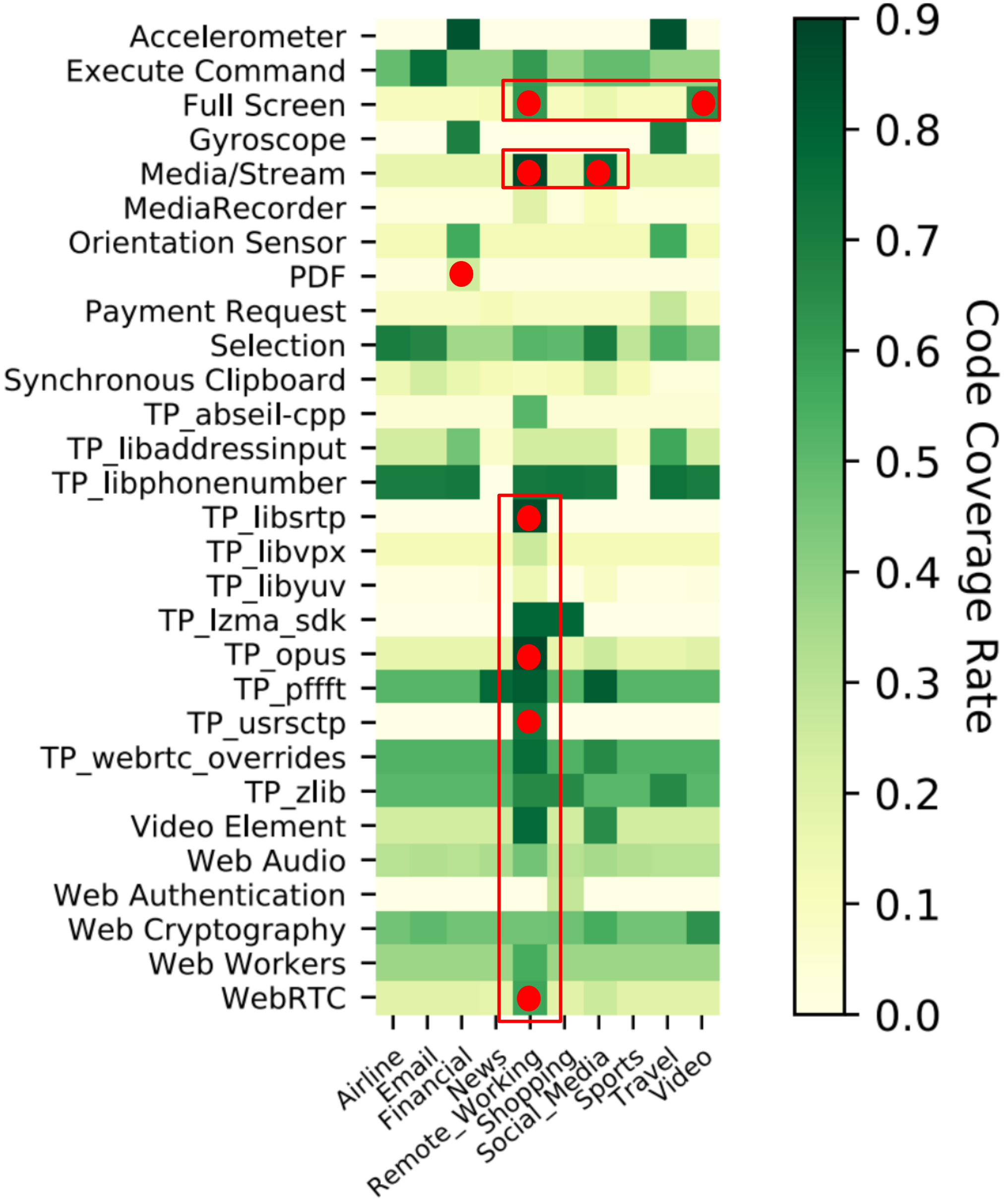
- Code Reduction & Security Benefits
  - Visit 40 websites from 10 different groups.



Category	Websites	User Activities	Code Reduction Size (MB)	Code Reduction Rate (%)	Number of Removed CVEs
Airline	aa, delta, spirit, united	Login; search a flight; make a payment; cancel the flight, logout.	24.17	53.8	97
Email	gmail, icloud, outlook, yahoo	Login; read/delete/reply/send emails (with attachments); open attachments; logout.	23.75	52.9	97
Financial	americanexpress, chase, discover, paypal	Login; check a statement; pay a bill; transfer money; logout.	23.45	52.2	91
News	cnn, cnbc, nytimes, washingtonpost	Read breaking news; watch videos; search other news.	24.19	53.9	98
Remote Working	bluejeans, slack, webex, zoom	Schedule a meeting; video/audio chat; share a screen; end the meeting.	18.57	41.4	81
Shopping	amazon, costco, ebay, walmart	Login; track a previous order; look for a product; add it to the cart; checkout; logout.	24.33	54.2	98
Social Media	instagram, facebook, twitter, whatsapp	Login; follow/unfollow a person; write a post and comment; like a post; send a message; logout.	23.30	51.9	93
Sports	bleacherreport, espn, nfl, nba	Check news, schedules, stats, and players.	24.39	54.3	98
Travel	booking, expedia, priceline, tripadvisor	Login; search hotels; reserve a room; make a payment; logout.	24.16	53.8	97
Video	amazon, disneyplus, netflix, youtube	Search a keyword; play a video (forward/pause/resume); switch screen modes (normal/theatre/full) ; adjust a volume	24.18	53.9	93
All	–	–	17.43	38.8%	73

Evaluation

- Feature Usages



Related Works

- Snyder’s work at CCS’17
  - “Most Websites Don’t Need to Vibrate: A Cost-Benefit Approach to Improving Browser Security”
  - Scope
  - API blocking vs Code removing

Limitations

- Rely on manual analysis.
- Not 100% guaranteed stable.

Questions?