How unique is your web Browser?

Peter Eckersley

PETS'10 Proceedings of the 10th international conference

presentation by:

Anshuj Garg(2011MCS2572)
Shehbaz Jaffer(2011MCS2578)

Instructor:

Prof. Huzur Saran

INTRODUCTION

- Tracking browser activity on a computer – cookies.
- Cookies disabled?
- Super Cookies.
- Super Cookies disabled?
- Browser fingerprinting.

BROWSER FINGERPRINTING

- Browser Fingerprinting
  - when a web browser sends a request it has few special parameters
  - These can be used to track the web browser activity.

Information extracted from Browser Request - I

Browser Characteristic	value
User Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:16.0) Gecko/20100101 Firefox/16.0
HTTP_ACCEPT Headers	text/html, */* gzip, deflate en-US,en;q=0.5
Browser Plugin Details	Plugin 0: DivXÂ® Web Player; ... librhythmbox-itms-detection-plugin.so;
Time Zone	-330

Information extracted from Browser Request - II

Browser Characteristic	value
Screen Size and Color Depth	1366x768x24
System Fonts	KacstFarsi, TeXGyreCurso... KacstBook (via Flash)
Are Cookies Enabled?	Yes
Limited supercookie test	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No

DEGREE OF ANONYMITY ACHIEVED PER ATTRIBUTE

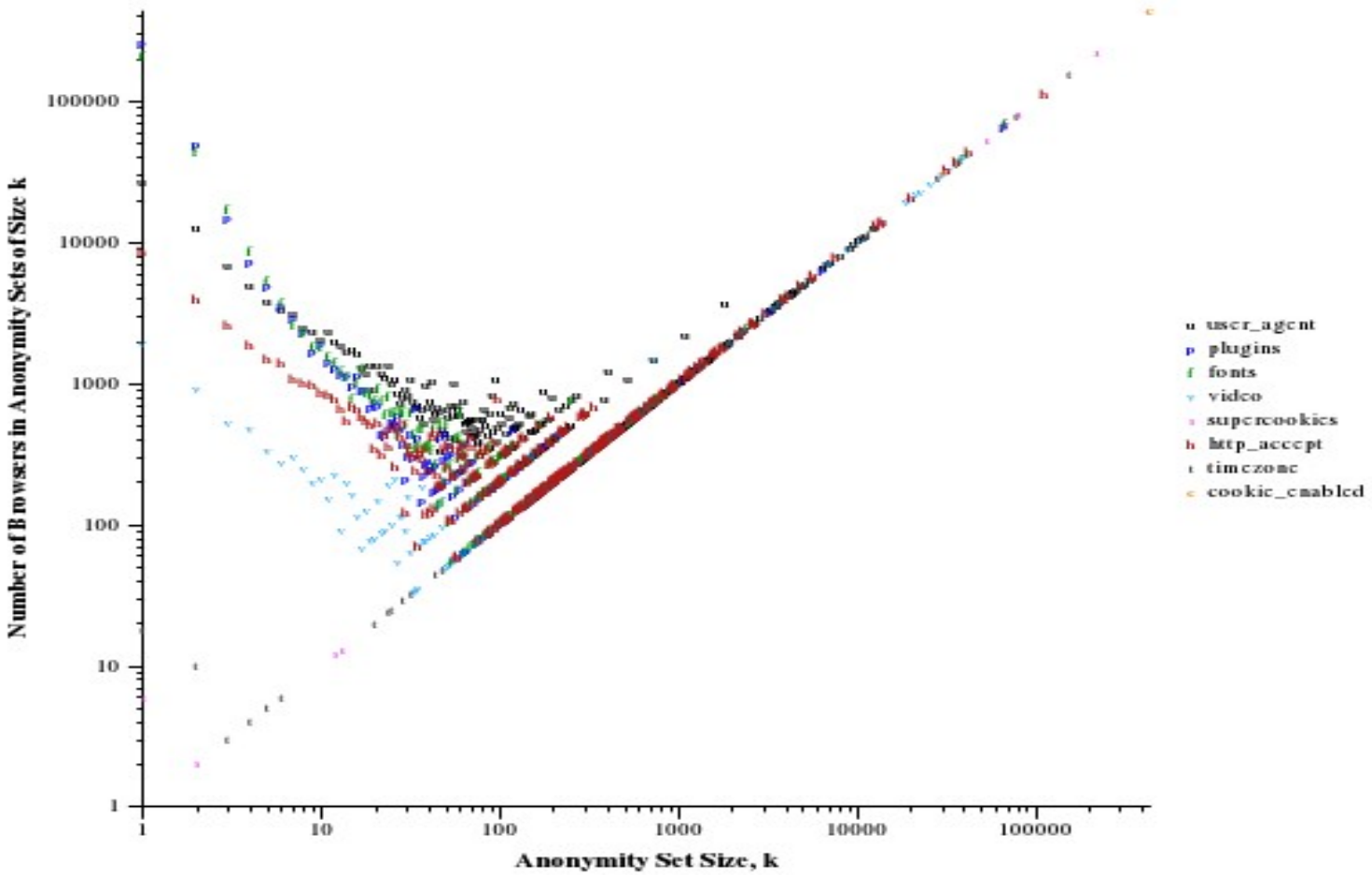


Fig. 3. Number of users in anonymity sets of different sizes, considering each variable separately.

BROWSER FINGERPRINTING

- Browser fingerprint
  - collect the browser parameters.
  - group them in strings.
  - concatenation of these strings gives the browser fingerprint.
  - if we pick a browser at random at best 1 in 286,777 browsers may share its fingerprint.
  - (experiment carried out on 470,161 browsers).

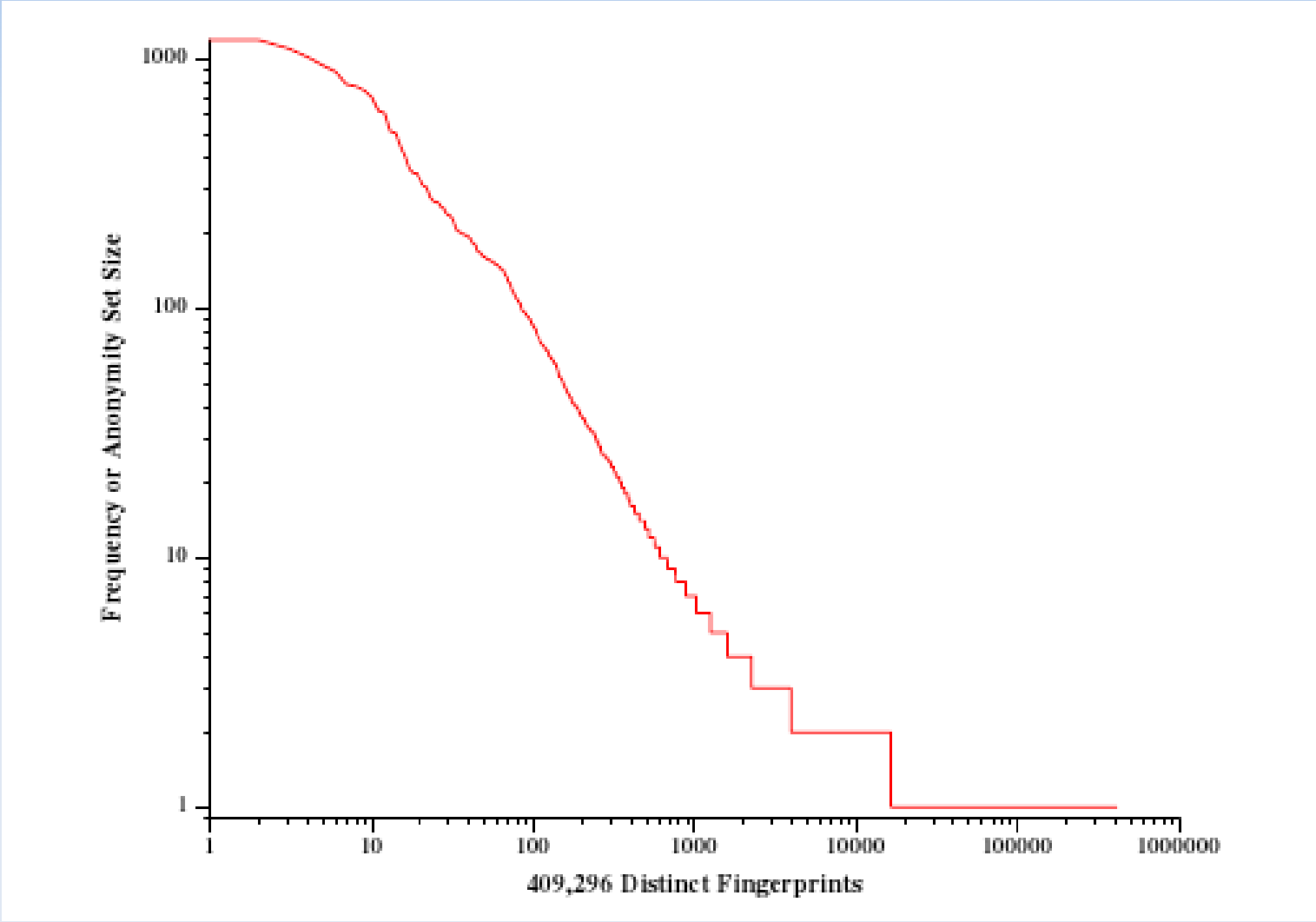
FINGERPRINT- THREAT TO WEB PRIVACY

- Fingerprints can be used as global identifiers for small set.
- Fingerprint + IP address can be used as cookie regenerators.
- Fingerprint + IP address without cookies.

UNIQUENESS IN BROWSER FINGERPRINT

- Javascript- attributes for video, plugins, fonts, super cookies.
- Flash add-ons – different for different browsers.
- Upgrading Browser plugins.
- Disabling Cookies.
- External monitor for altering screen resolution.

FINGERPRINT DISTRIBUTION



THE EXPERIMENT

- Kept track of HTTP request using HMAC and IP address.
- False positive elimination.
- Firewall filtering.
- User agent filtering.
- Browser fingerprint update detection.

BROWSER FINGERPRINT UPDATE DETECTION

Algorithm 1 guesses which other fingerprint might have changed into q

```
candidates ← []
for all g ∈ G do
  for i ∈ {1..8} do
    if for all j ∈ {1..8}, j ≠ i : F_j(g) = F_j(q) then
      candidates ← candidates + (g, j)
    end if
  end for
end for
if length(candidates) = 1 then
  g, j ← candidates[0]
  if j ∈ {cookies?, video, timezone, supercookies} then
    return g
  else
    # j ∈ {user_agent, http_accept, plugins, fonts}
    if SequenceMatcher(F_j(g), F_j(q)).ratio() < 0.85 then
      return g
    end if
  end if
end if
return NULL
```

`difflib.SequenceMatcher().ratio()` is a Python standard library function for estimating the similarity of strings. We used Python 2.5.4.

CHANGING FINGERPRINTS

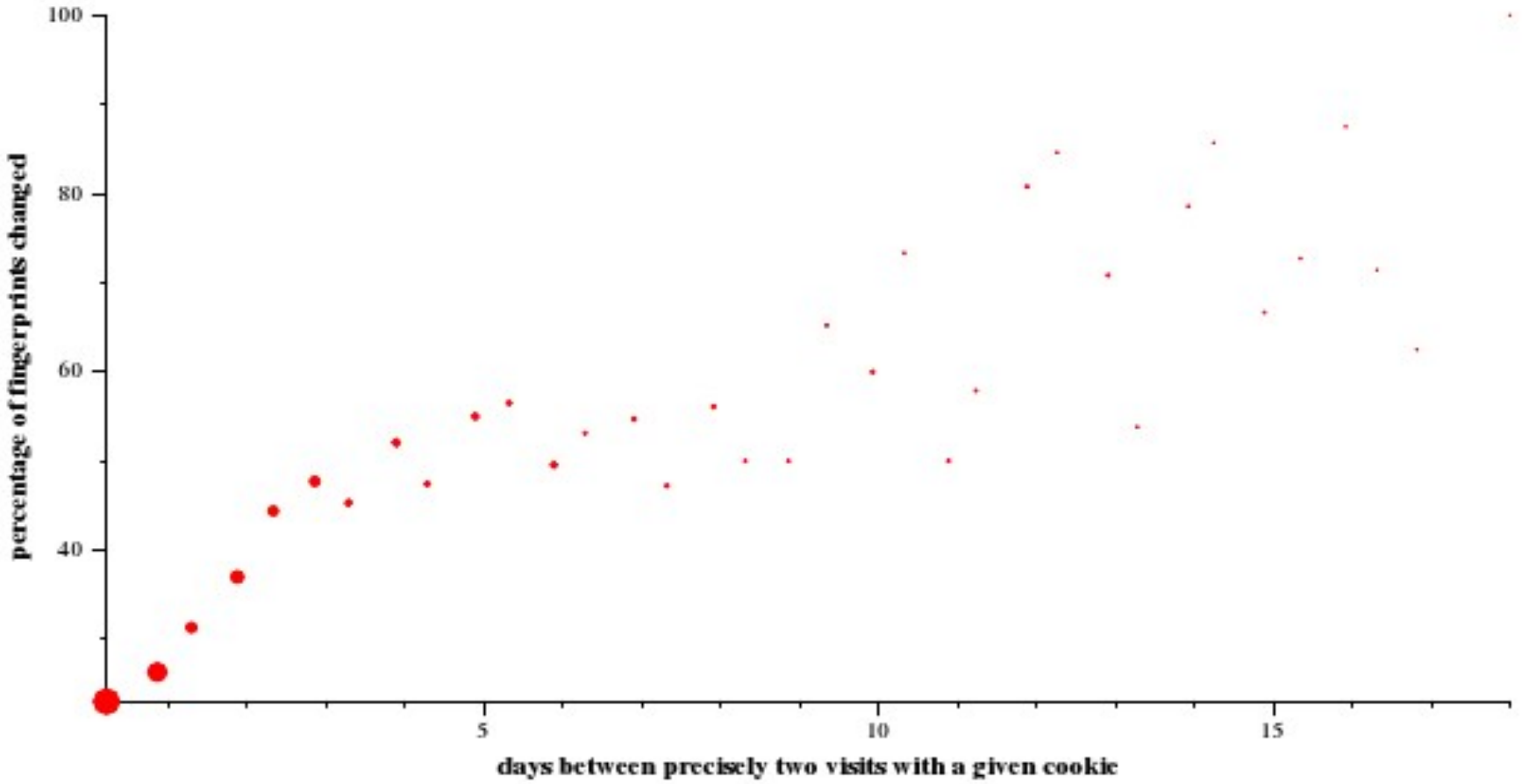


Fig. 4. Proportion of fingerprints that change over given intervals (area of datapoints indicates number of observations encompassed, $N = 4{,}638$)

DEFENCE AGAINST FINGERPRINTING

- The current defenses makes the browser fingerprint more unique.
  - user agent spoofing.
  - flash blocking.
- Important factor with respect to web privacy and user trackability.

REFERENCES

- **Peter Eckersley**, How Unique Is Your Web Browser? PETS Privacy Enhancing Technology and Security.

Thank You