Tales of Favicons and Caches: Persistent Tracking in Modern Browsers

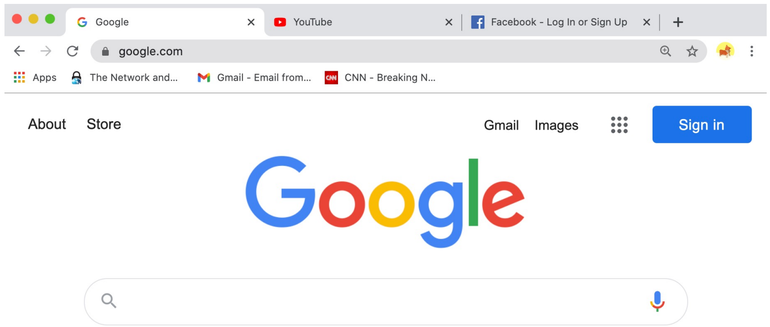
Konstantinos Solomos, John Kristoff, Chris Kanich, Jason Polakis
University of Illinois at Chicago, USA
ksolom6@uic.edu

NDSS SYMPOSIUM/2021

UIC

What is a Favicon?

- Introduced in Internet Explorer 5, 1999
    - ”Favorite website icon” → Favicon
    - Small icon associated with a webpage



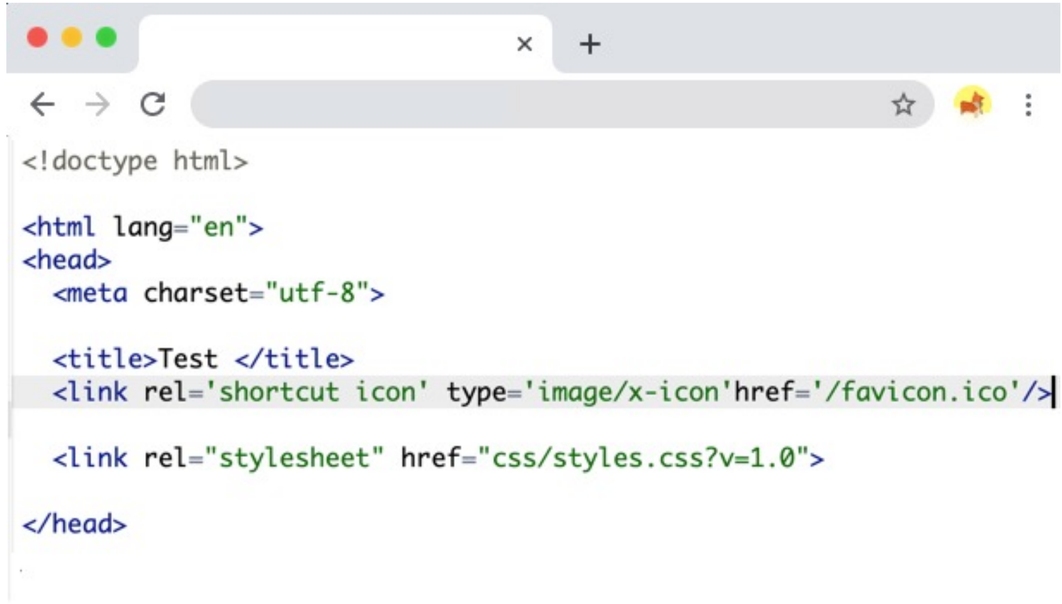
- Different icon formats
- Supported by all browsers and devices
- Part of websites’ branding identity

Favicon Storage & Cache

- Automatically requested and fetched

- **Dedicated Favicon Cache**

  1. Page URL
  2. Favicon ID
  3. Expiration Time (TTL)
  4. Dimensions



Favicon Cache Policies

ID	Page URL	Favicon ID	TTL	Dimensions	Size
1	foo.com	favicon.ico	5000	16x16	120
2	abc.foo.com	icon.png	1000	32x32	240
3	foo.com/path	favicon2.ico	25000	16x16	180

1. Requirements for creating an *entry*
    I. Favicon not already exists
    II. Favicon URL is valid
    III. Icon renders properly

Favicon Cache Policies

ID	Page URL	Favicon ID	TTL	Dimensions	Size
1	foo.com	favicon.ico	5000	16x16	120
2	abc.foo.com	icon.png	1000	32x32	240
3	foo.com/path	favicon2.ico	25000	16x16	180

2. Subdomains and inner paths create different entries

Favicon Cache Policies

ID	Page URL	Favicon ID	TTL	Dimensions	Size
1	foo.com	favicon.ico	5000	16x16	120
2	abc.foo.com	icon.png	1000	32x32	240
3	foo.com/path	favicon2.ico	25000	16x16	180

3. Access Control

- Incognito mode can read and not write

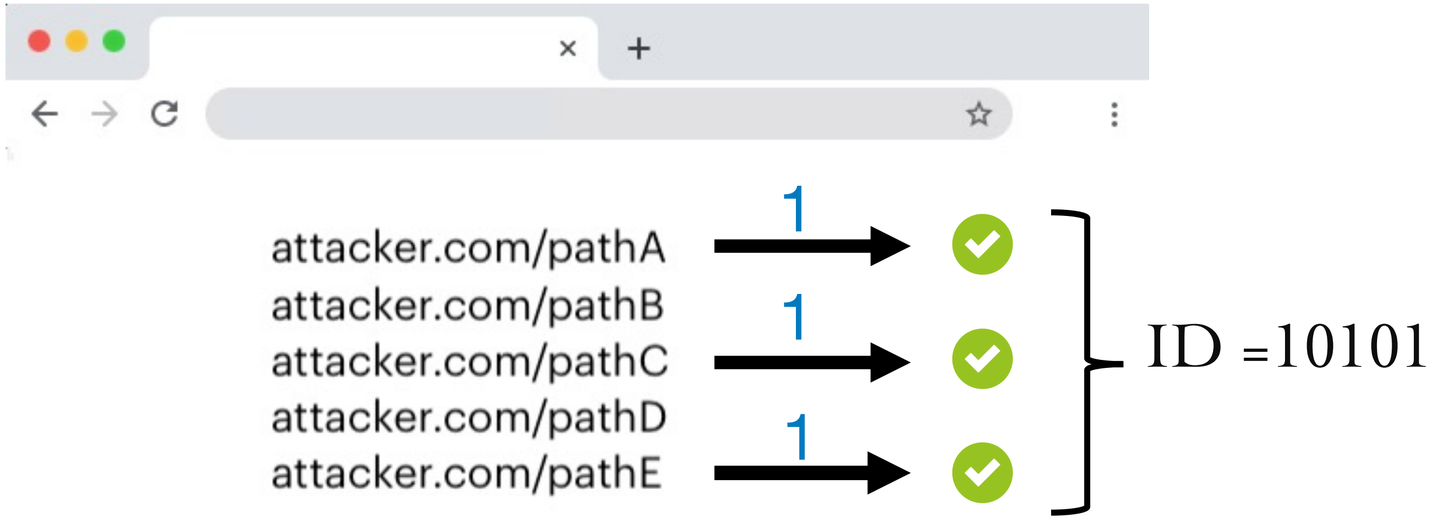
Favicon Supercookie

- Leverage favicons to create **persistent tracking identifier** for user across visits

- Attacker website
  1. Encodes chain of subpaths as a vector : <pathA, pathB, pathC , pathD>
  2. Serves different favicons for each path : <iconA, iconB, iconC, iconD>
  3. Stores browser identifier as favicon cache entries

Threat Model

Victim visits website and the identifier is automatically stored

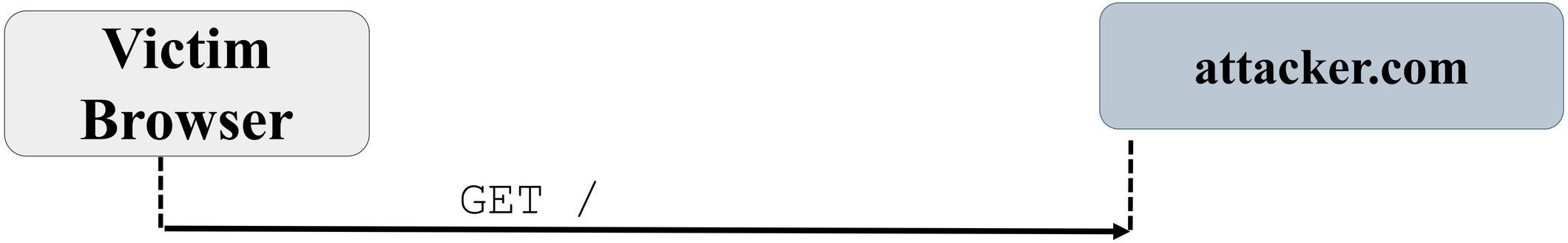


Write Identifier

Victim Browser

attacker.com

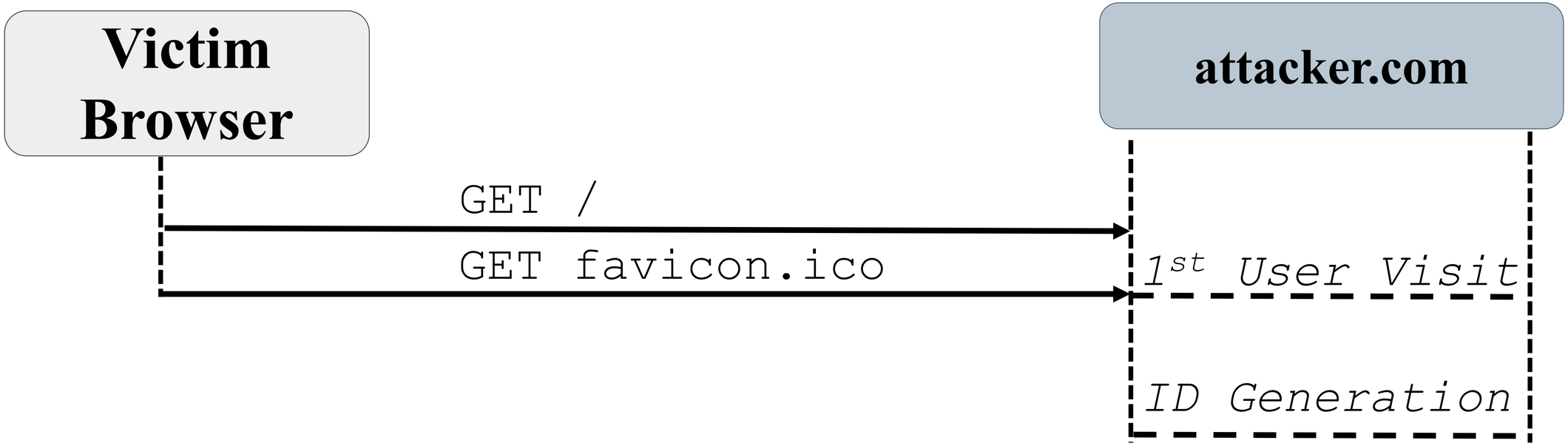
Write Identifier



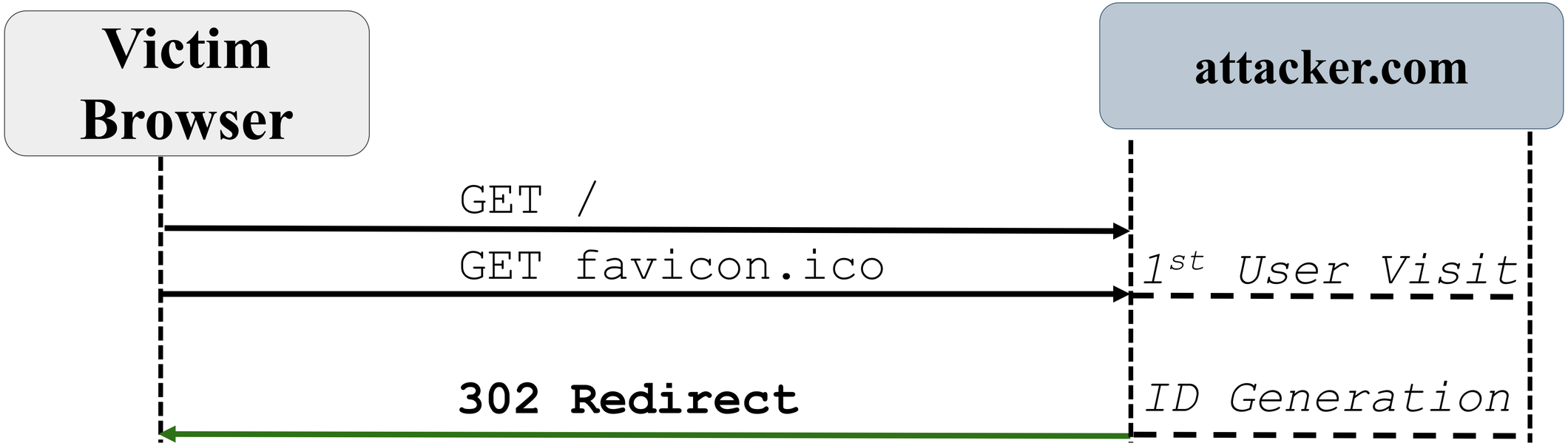
Write Identifier

Write Identifier

Write Identifier



Write Identifier

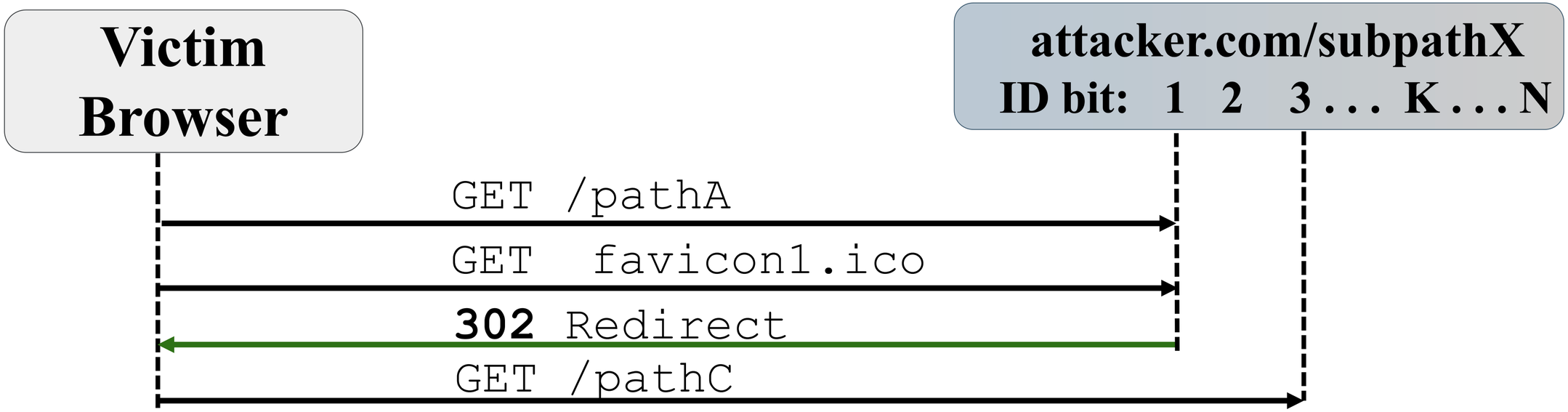


Write Identifier

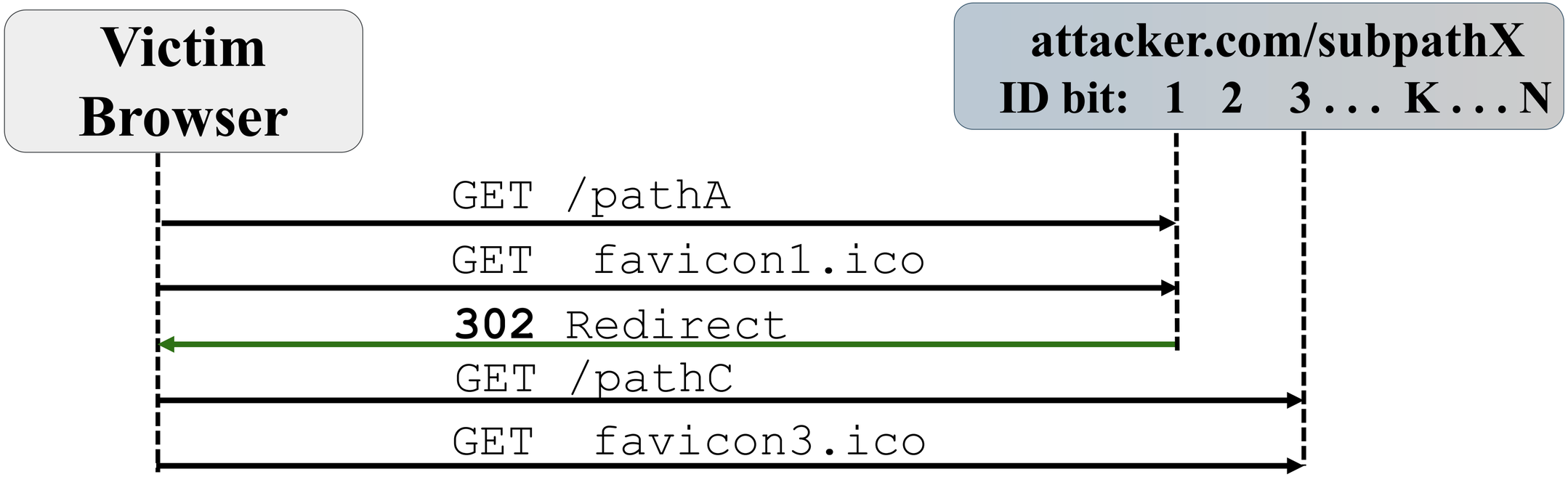
Write Identifier

Write Identifier

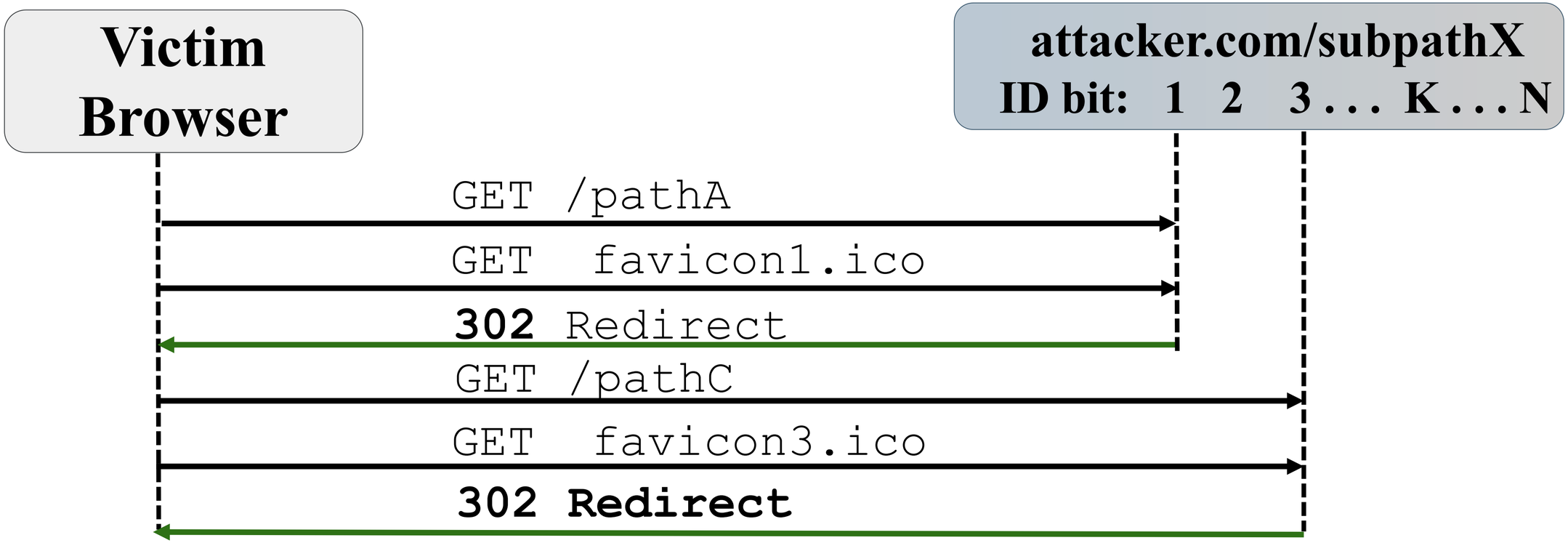
Write Identifier



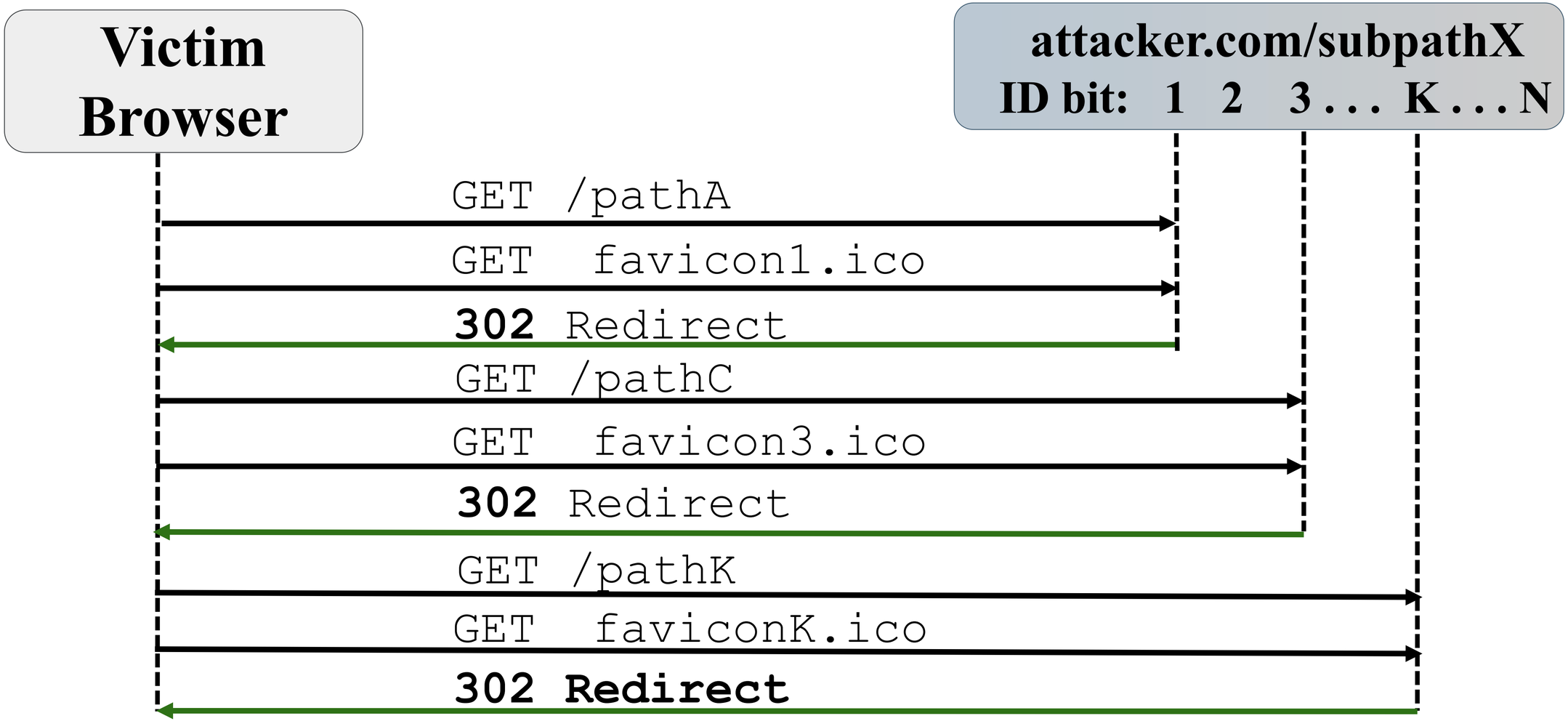
Write Identifier



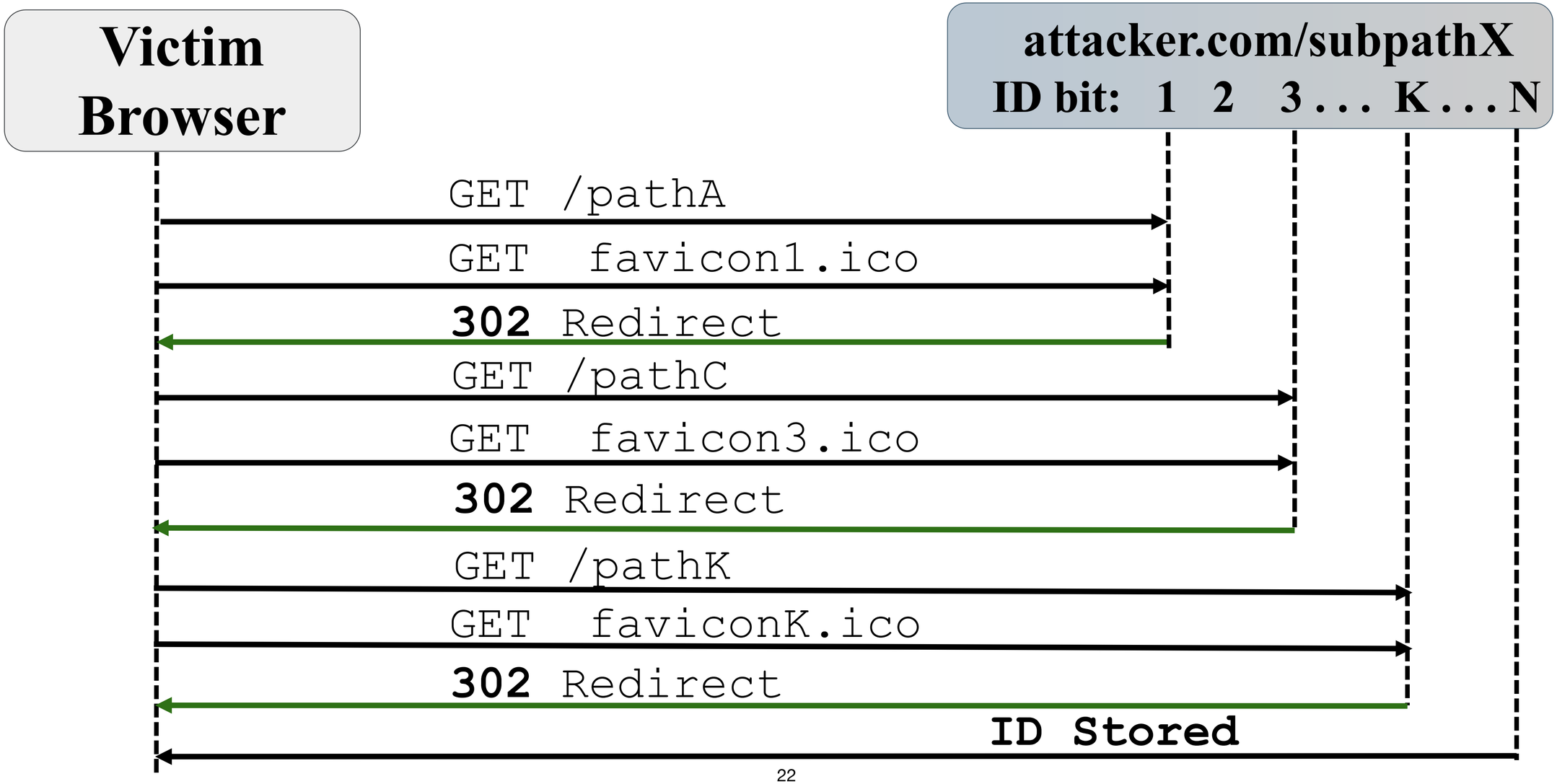
Write Identifier



Write Identifier



Write Identifier

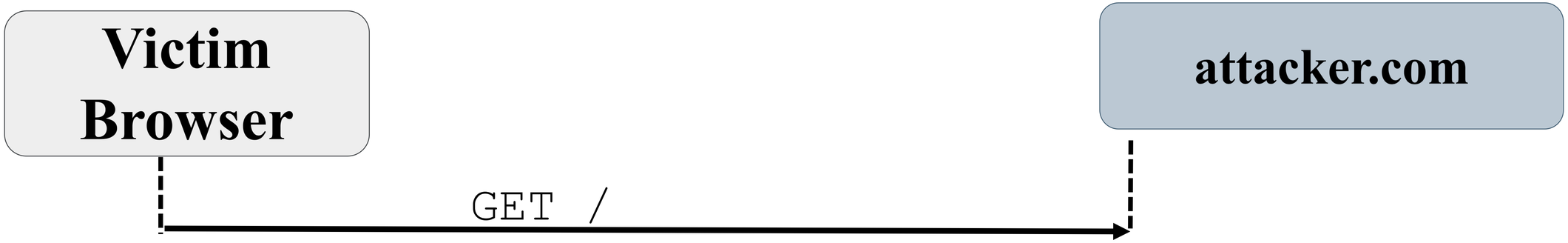


Read Identifier

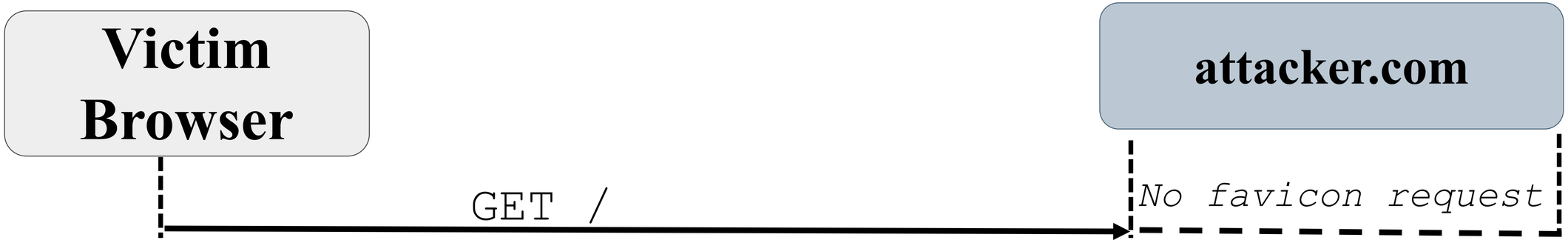
Victim Browser

attacker.com

Read Identifier



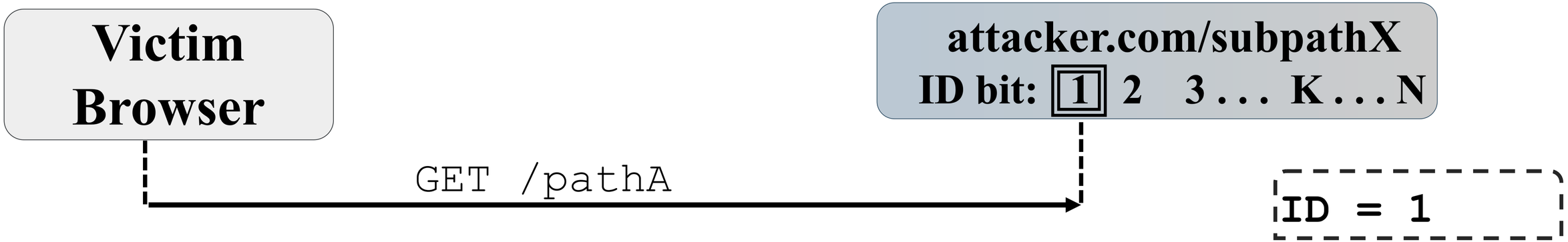
Read Identifier



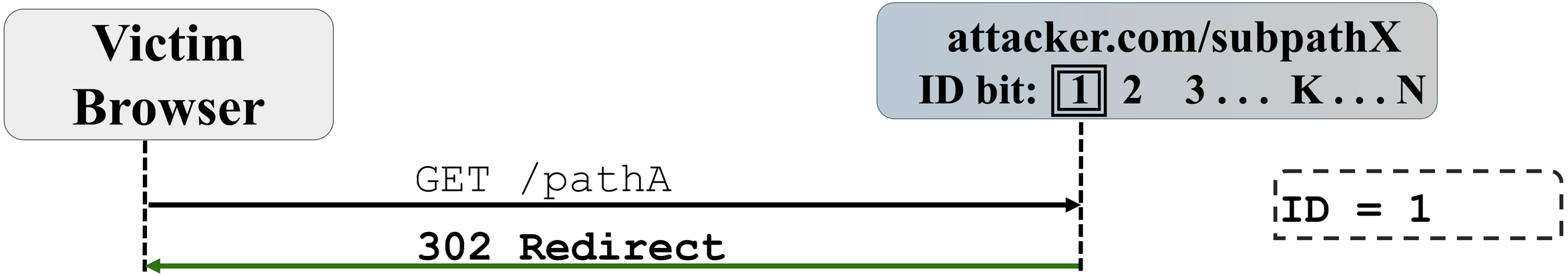
Read Identifier

Read Identifier

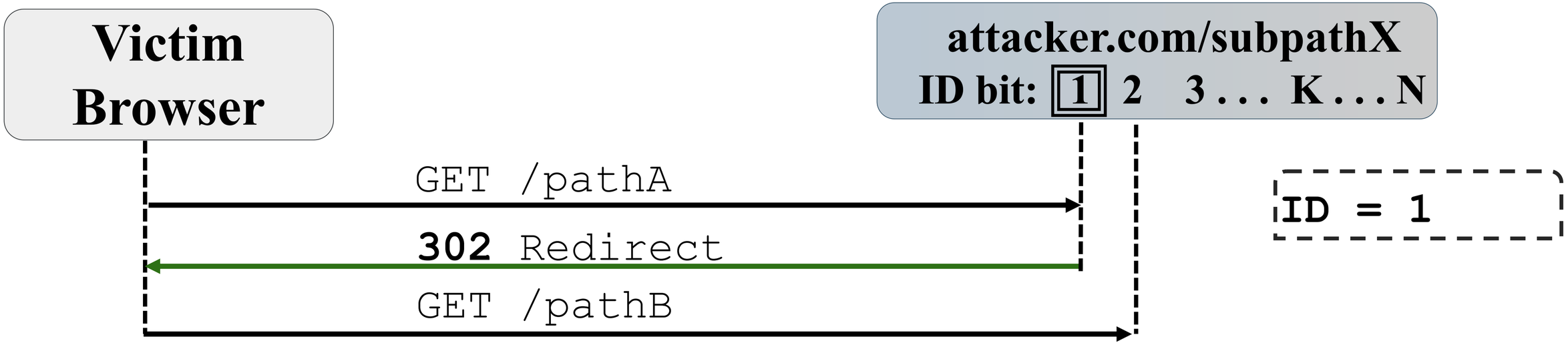
Read Identifier



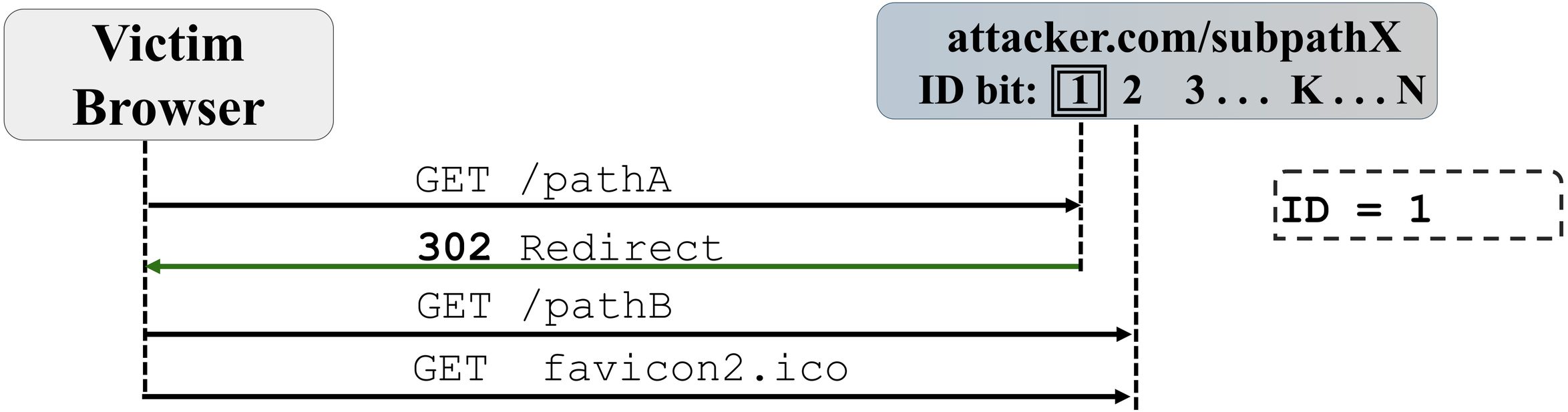
Read Identifier



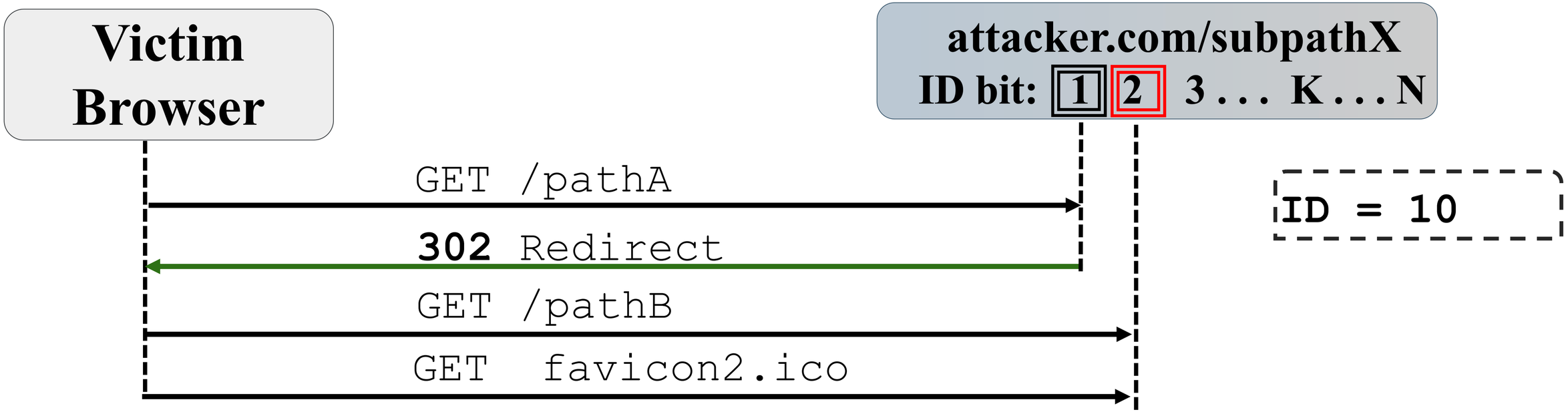
Read Identifier



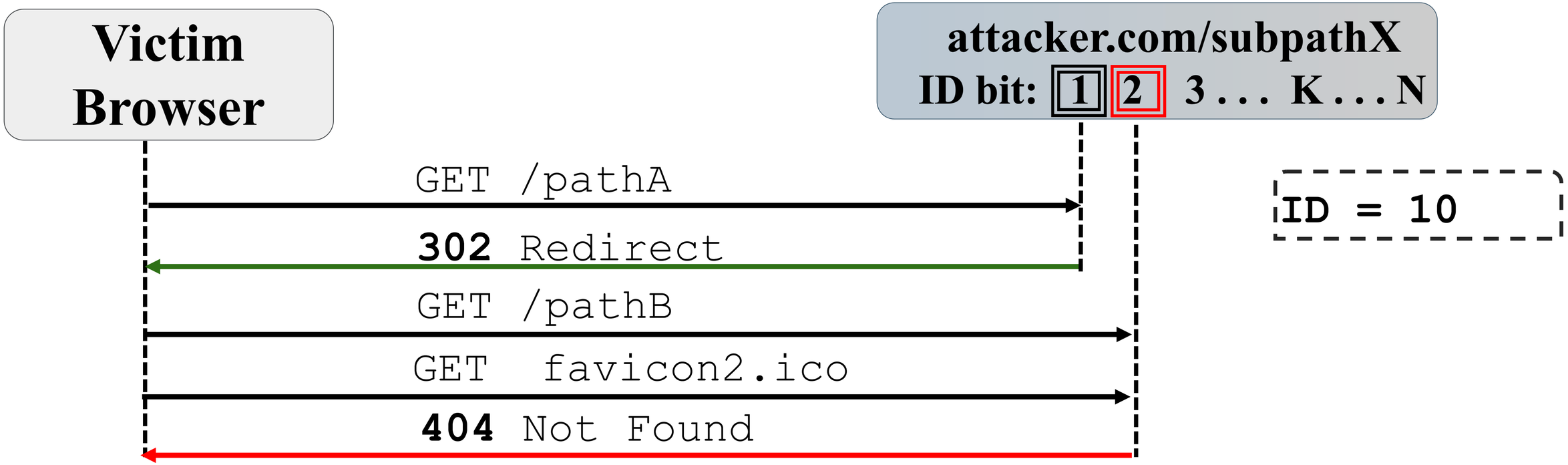
Read Identifier



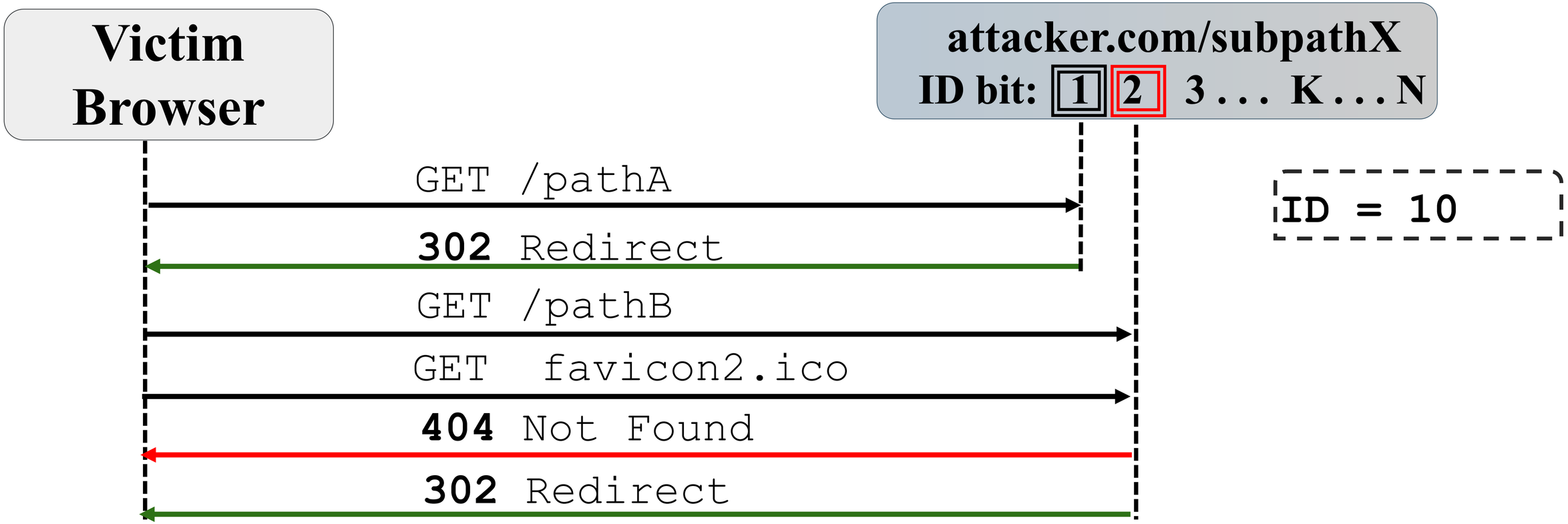
Read Identifier



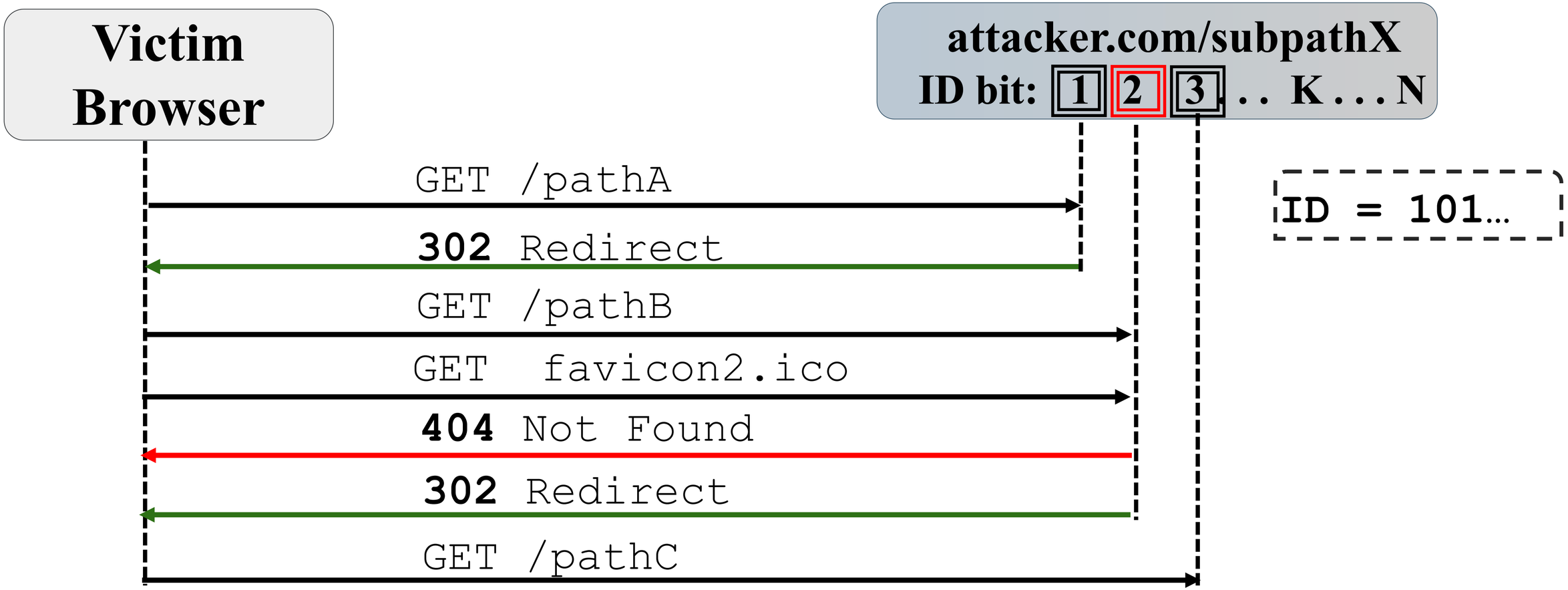
Read Identifier



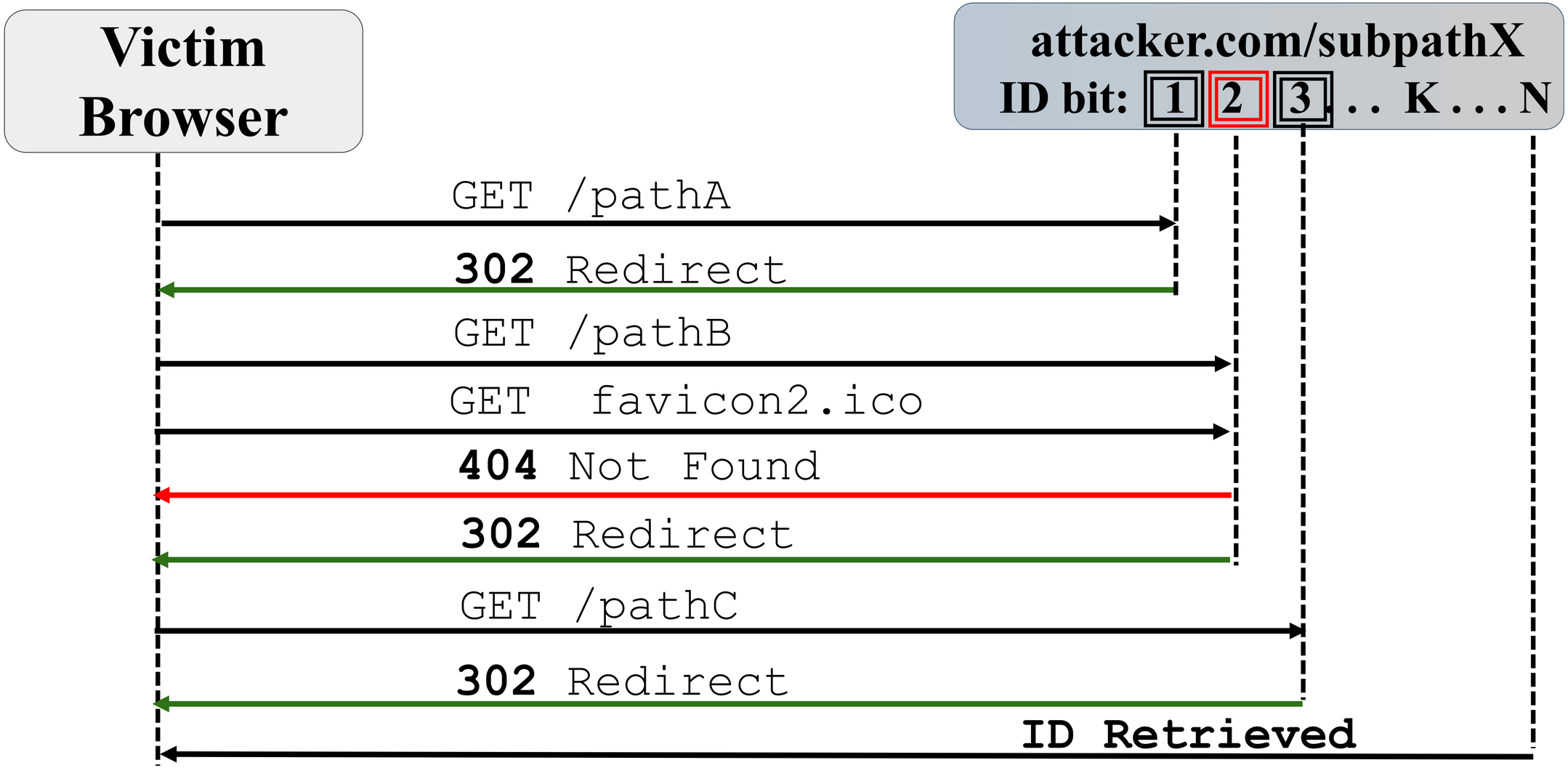
Read Identifier



Read Identifier



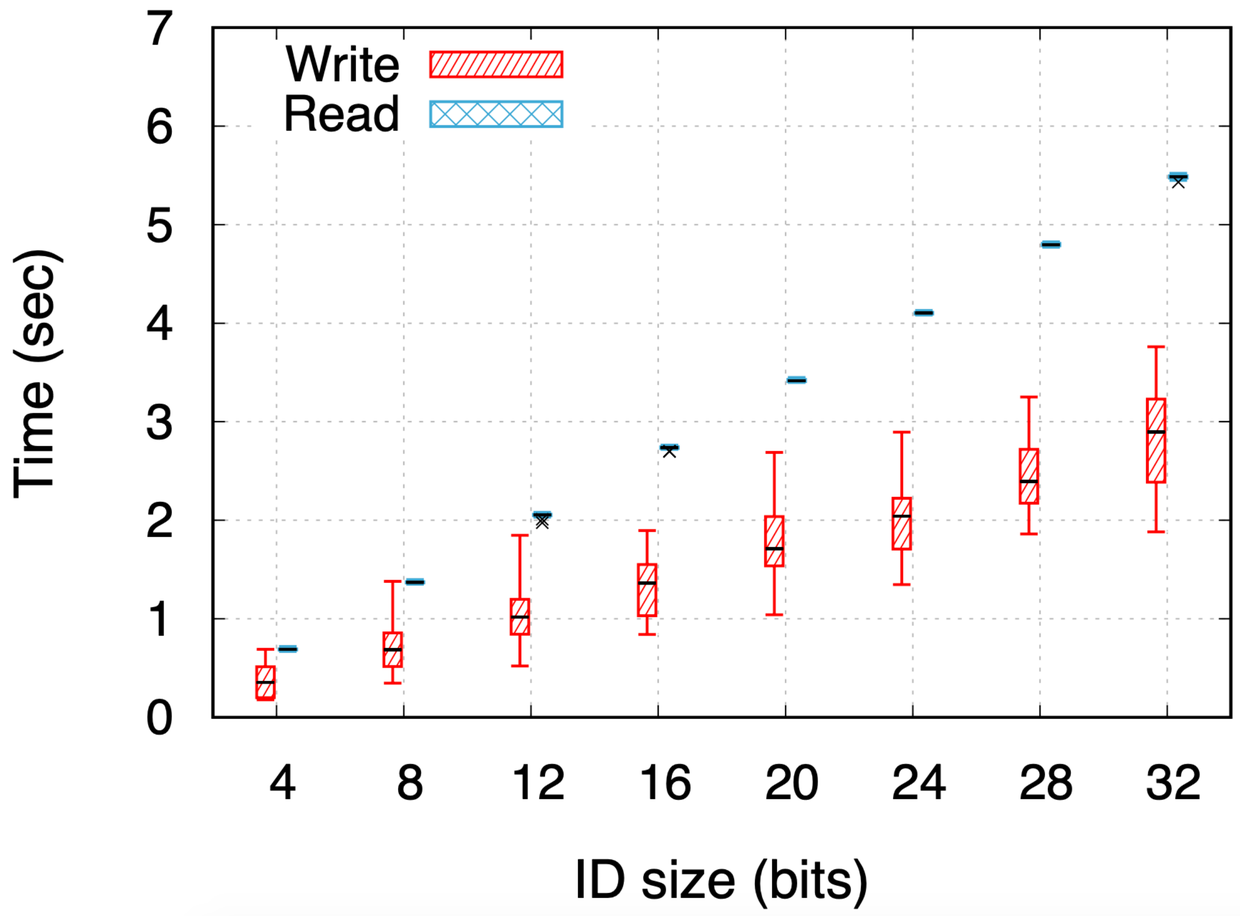
Read Identifier



Affected Browsers and Modes

	Incognito	Clear Browser Data	Anti-Tracking Extensions	VPN
Chrome	✓	✓	✓	✓
Safari	✓	✓	✓	✓
Edge	✓	✓	✓	✓
Brave	✓	✓	✓	✓

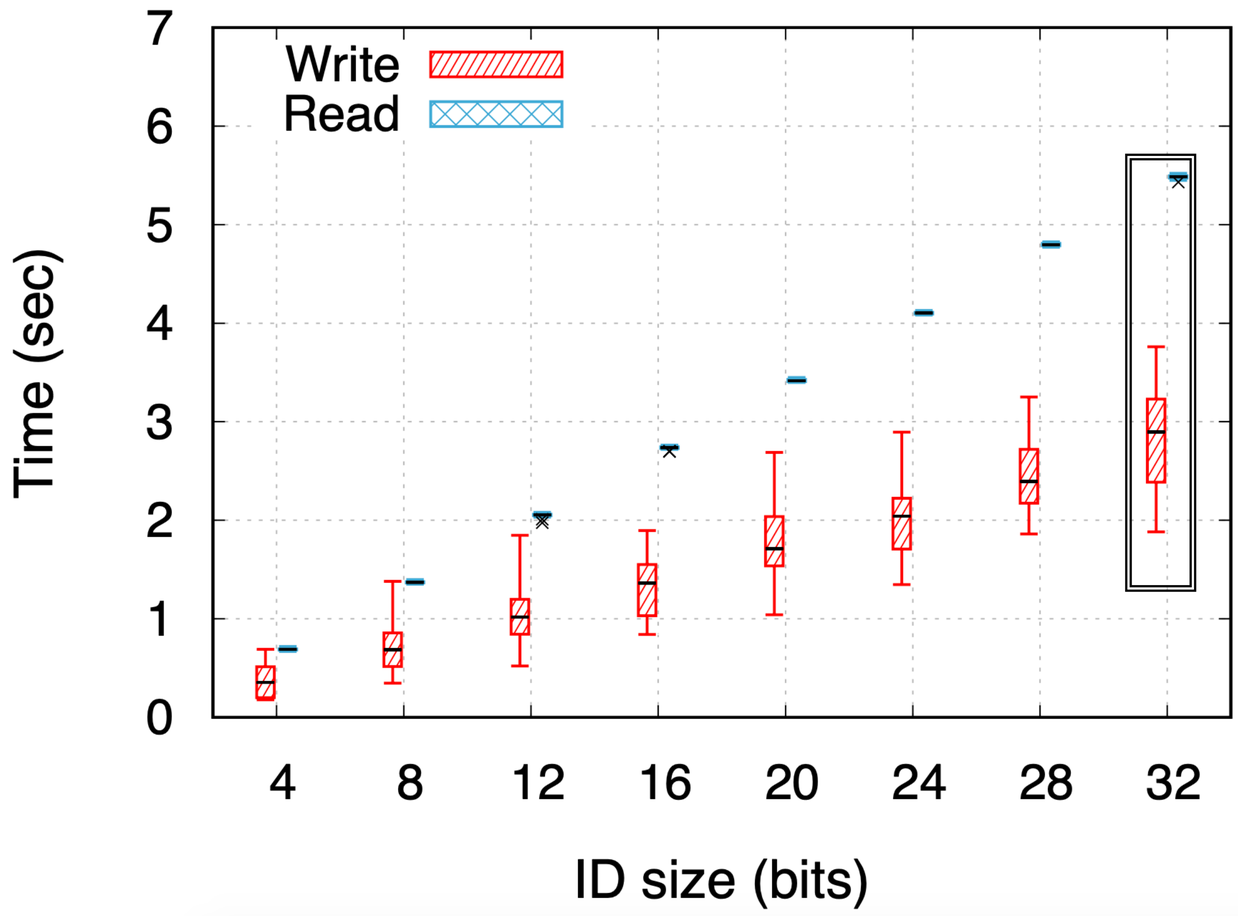
Baseline Attack Performance



- Write Identifier ≤ 2.5 sec
- Read Identifier ≤ 5.5 sec
- Average tracker overhead ≥ 10 sec [M. Hanson et al.,Tech.Rep.18’]

➢ **Can we do better?**

Baseline Attack Performance



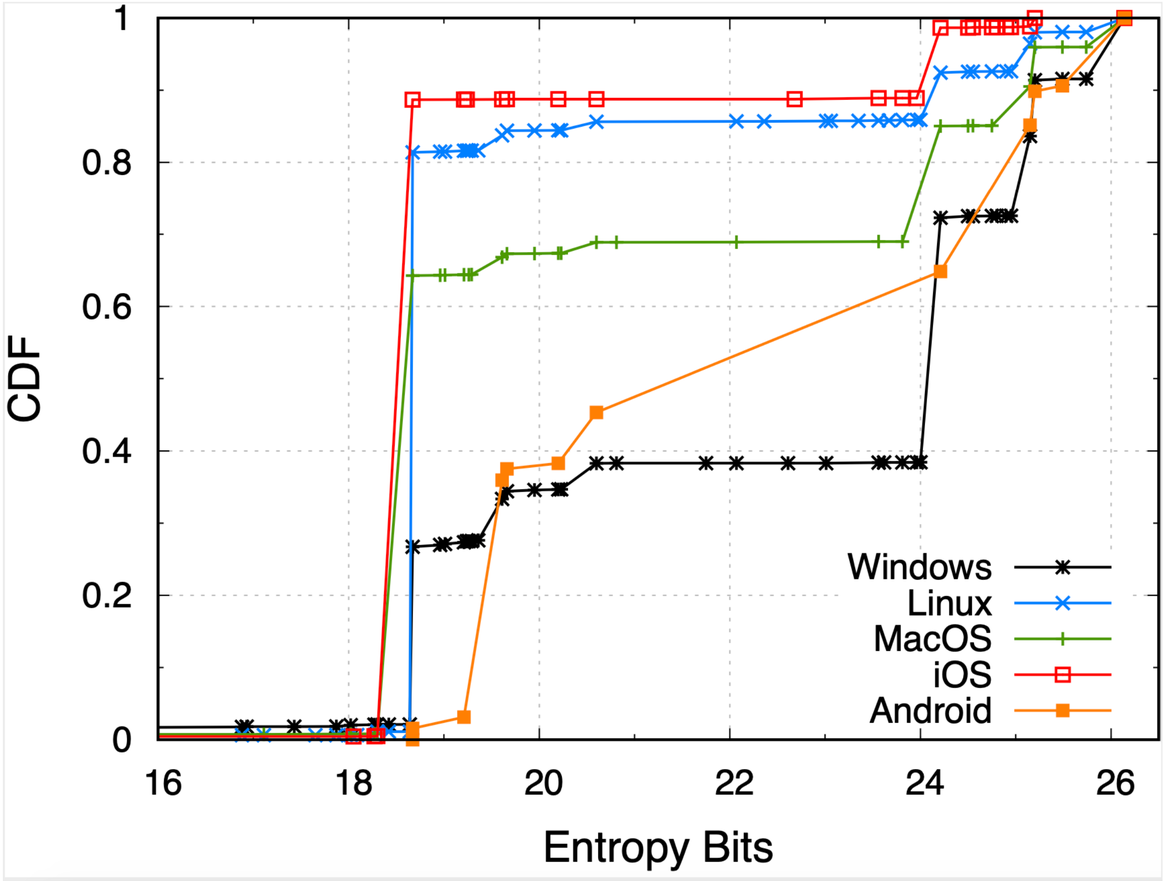
- Write Identifier ≤ 2.5 sec
- Read Identifier ≤ 5.5 sec
- Average tracker overhead ≥ 10 sec [M. Hanson et al.,Tech.Rep.18’]

➢ **Can we do better?**

Optimization: Fingerprints and Favicons

- Browser attributes that are immutable over time [Vastel et al., S&P 18’]
  - `Cookies Enabled, Local Storage, DNT, Ad Block, Platform, Encoding, Language, WebGL ,Canvas`
- Browser Fingerprint dataset `amiunique.org` [Lapperdrix et al.,S&P 16’]
  - Calculated Fingerprint Entropy of the available attributes

Optimization: Fingerprints and Favicons



- Lower: **16 bits**
- Higher: **26 bits**
- 50% desktop devices: **19-24 bits**

➢ **Combine Browser Fingerprint with Favicon Identifier**

Optimization: Fingerprints and Favicons

- Fingerprint generation overhead **≤ 200** ms
    - Cookies, Local Storage, DNT ≤ 2 ms
    - Canvas, WebGL ≤ 100 ms
- Reconstruct 32-bit ID with less redirections
    - **20 bits** Browser FP + **12 bits** Favicon ID ≈ **2 sec**
- Anti-Fingerprint tools
    - Randomize WebGL- Canvas: **18** bits
    - Brave defense: **12** bits → Full ID reconstruct ≈ **3 sec**

Network Effects

- Web server and client located in the same city
    - **27%** faster ID Generation
    - **35%** decreased read-ID time
- **Optimal** attack time with redirection overhead
    - Write ≈ **1.5 sec** – Read ≈ **3 sec**

➢ Large-Scale attack: dedicated CDNs and servers across locations

Proposed Countermeasures

1. Incognito mode should use an isolated cache instance
2. Default “Clear browsing data” should also clear Favicon Cache

- Notified vulnerable browsers
  - Confirmed and acknowledged
  - Brave deployed countermeasure

Summary

- Demonstrated novel persistent favicon tracking technique
  - Breaks incognito mode
  - Robust against anti-tracking defenses
  - Long-term identifier
- Browser FPs a powerful optimization mechanism for augmenting other tracking vectors
- Extensive experimental evaluation under different network/device/browser conditions
- Mitigation needs redesign of policies and browser architecture. Remediation under way.

Thank you!

Feel free to reach out with any questions:

ksolom6@uic.edu