Live Exercises

Online tracking

(adapted from a previous exam question)

Tracking Alice

In class, you have seen various techniques to track users online.

- Alice browses a website selling shoes. Later, she noticed that many ads she sees on different websites are advertising for shoes. How is this happening ?

- After learning about online tracking using cookies, Alice decides to completely **disable cookies** in her browser.
  Does this make Alice anonymous?
  How can an adversary website still identify and track Alice ?

Defense against browser fingerprinting

As a computer scientist, you want to help Alice remain anonymous while she browses the internet.
So you want to deploy a defense against browser fingerprinting at the client's browser side based on a **"detect & block" strategy.**

- **How** would you design your solution?
  How does it work?

- What are the **drawbacks** of the solutions you proposed?

Propose another defense strategy

Another approach against browser fingerprinting is **modifying the browser's behavior** with respect to different protocols and APIs in order to break the fingerprints (e.g., modifying the standard User-Agent string, or canvas behavior).

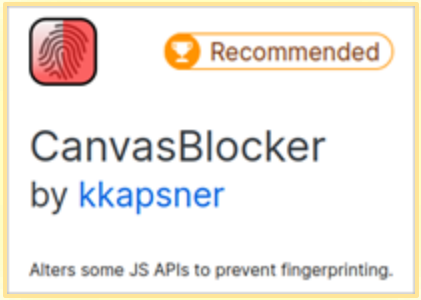
Describe one defense strategy against browser fingerprinting that leverages this approach.

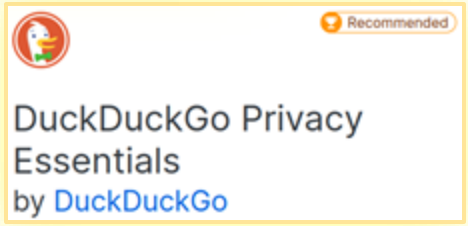
- How would you modify the browser behavior, and why does it prevent browser fingerprinting?
- List at least one potential drawback of the method in terms of either protection or utility.

Propose another defense strategy

Is loss of utility really a big deal ? Just generalize !

There are even browsers extensions to do so !





It looks like nothing,
But nothing looks like it !