PRI - Web Tracking Tutorial

During this 3 hours tutorial, you will explore the reach of web tracking methods, and countermeasures to avoid them. This tutorial proposes guided steps and tips, but you can do manipulations multiple times and use external sources to get more information. Do not forget to revert your changes between each section, in order to use **one countermeasure at a time**. Do not hesitate to ask questions or comment the obtained results.

Manipulations will be done using the Firefox browser, which last version is available here. We suggest you to use another browser profile, or even computer profile, if you already use Firefox as default browser. Please **deactivate any web tracking blocking tool** if you already have one, just the time of this tutorial, you can activate them afterward.

Cookies

In this section, we will take a look at the cookies and countermeasures to avoid their use for web tracking purpose. First, we will look at the cookies that are stored in the web browser.

1. Open the web development console (`toolbar > tools > web development`).
2. Navigate to the website of your choice in order to see which cookies it stores on your browser. *A list is proposed below if you have no idea.*
3. Go to `Storage` section. *Here you can see each storage mechanism with the data it holds for the current domain.*
4. Into the `Cookies` category, you will find the cookies that are stored for the current domain.
5. Identify those belonging to a first party, and those of third parties.

Lightbeam

Lightbeam is a Firefox extension that allows to save a graph of each visited domain, linked to any third party included on them.

1. Download and install the extension.
2. Navigate on the web. *Try on your favorite websites, or on some proposed below, the more (diverse) the better.*

Here is a list of websites you can browse :

- https://news.google.com (aggregated news)
- https://www.huffingtonpost.com (news)
- https://www.cnn.com (news)
- https://www.washingtonpost.com (news)
- https://www.univ-rennes1.fr (university)
- https://www.qwant.com (privacy conscious search engine)
- https://en.wikipedia.org/wiki/Internet_privacy (wikipedia)
- https://www.facebook.com (social networks)
- https://www.twitter.com (social networks)

1. Click on the extension logo to open the visualization.
2. Which type of browsing profile can third parties have about you ?
3. Are every third party an advertisement service provider ? Does one offer another type of service ?
4. Revert your changes by deactivating the extension.

Private browsing mode

1. Open a private browsing mode window.
2. Open simultaneously a web page in normal browsing and private browsing mode. Are cookie values the same ?
3. How do you explain this ? *We suggest you to look at the Content blocking Firefox feature.*
4. Which type of countermeasure strategy is used ? Which entity provides it ?
5. You can now go back to normal navigation mode.

Behavioral detection

Privacy Badger is an extension offered by the EFF, that detects trackers by their behaviour, instead of using a black list.

1. Install the extension.
2. Navigate some more on the web, and also on the news websites proposed above. On each visit, open the extension's popup.
3. Do you see a change in the classification of domains ? If yes, when did it occur ?
4. Are some domains marked in orange ? Why ? *You can look for an answer here.*
5. Revert your changes by deactivating the extension.

Evercookie

The original evercookie project is available on Samy Kamkar's website. On it, you will find a description of methods used to store the evercookie, with a tool to play with it.

1. Generate an evercookie in your browser by clicking on the corresponding button (first one in EXAMPLE section). *Do not worry, it cannot be used for tracking, see the description for more information.*

Manual deletion

1. Open the web development console (`toolbar > tools > web development`).
2. Go to `Storage` section.
3. Find any instance of the evercookie (named `uid`) and delete all of them.
4. Now, rediscover the evercookie by clicking on the `Click to rediscover cookies WITHOUT reactivating deleted cookies` button (not the one above !).
5. Did it manage to discover the evercookie ? If yes, by which mechanisms ?

Private browsing mode

1. Open a private browsing mode window.
2. Try to rediscover the evercookie. Did it manage to rediscover it ?
3. You can exit the private browsing mode now.

Behavioral detection

1. Reactivate Privacy Badger.
2. Try to rediscover the evercookie. Did it manage to rediscover it ?
3. Do you think that it could in some particular contexts ?
4. Revert your changes by deactivating the extension.

Other information

IP address information

Other informations are sent by your browser when you browse the web. One of them is the IP address, which is needed in order to communicate with a server. But using this information, others can be infered.

1. Go to https://whatismyipaddress.com.
2. Which information could be inferred from your IP address ?
3. What level of precision does it have ?
4. Do you think that using these informations, we could track your very own browser ?
5. Do you think that you can evade this, and how ?

HTTP headers

Your browser also send HTTP headers alongside each request.

1. Open the developer console and go to `Network` panel.
2. Go to the website of your choice, and navigate to another page using a link present on the first one.
3. Select one of the request on the left panel.
4. On the right panel, go into `Headers` category, and scroll to find `Request headers` . *These are the HTTP headers sent by your browser for this request.*
5. Look closer at the `Referer` header, what does it contain ?
6. Which informations could leak through this field ?

Look at the other header fields, we will now look at how these other headers can be used for web tracking.

Browser Fingerprinting

In this section, we will look at how browser fingerprinting can be used for web tracking, and different countermeasure strategies to try to fight it.

1. Check your browser fingerprint on AmIUnique.
2. What is the size of your browser fingerprint's anonymity set size ?
3. Look at the details, and identify your browser's attributes values that are common, and those that are not.

We will now use countermeasures to avoid identification, and try to fall into a larger anonymity size. To easily compare your fingerprints, hold each fingerprinting result open into a distinct tab.

Private browsing mode

1. Open a window in private browsing mode and fetch your fingerprint.
2. Could a tracker still follow you in "private browsing mode" ?
3. You can go back to normal mode for the following parts.
4. Behavioral : Do you think that activating `Privacy Badger` would protect you from fingerprinting ?

Spoofing attribute value

User-Agent Switcher is the first tool that we will use. This extension allows you to change your User-Agent.

1. Install and activate this extension for the `amiunique.org` domain.
2. Now, replace your User-Agent by one of your choice. *You can pick one randomly, or choose one specifically. You can look at the statistics provided by AmIUnique or any other source.*
3. Fetch your fingerprint using this spoofed User-Agent, and compare your new User-Agent anonymity set size against the previous one.
4. What about your overall fingerprint ?
5. Revert your changes by deactivating the extension.

Randomization (1:N)

The tool that we will use is the Canvas Fingerprint Defender extension, which adds noise into each generated canvas.

1. Install and activate this extension.
2. Fetch your fingerprint a first time. Look at the canvas, can you distinguish the added noise ?
3. Save this first canvas on your disk as an image file.
4. Force the generation of a second fingerprint. Does the canvas on this one seems different to the precedent ?
5. Save this second canvas on your disk. *Do not rewrite the first one.*
6. Go to online-image-comparison.com, define the `fuzz` parameter to `1` and compare the two canvases.
7. Are the two canvases identical ? What about the whole fingerprint ?

8. Do you think that this strategy is applicable to other attributes ?
9. Revert your changes by deactivating the extension.

Standardization (N:1)

The best tool for defense by standardization is Tor Browser, as it seeks to have the exact same configuration on each installation. We will stick to the Firefox browser, which began to embark some, but they are still behind a flag.

1. Go to `about:config` , and accept to take the risk.
2. Search for the `privacy.resistFingerprinting` property.
3. Activate it by double clicking on it.
4. Fetch your fingerprint, how is your anonymity set ?
5. Have some attributes changed ? What do you think about that ?
6. Revert your changes by putting the property to its default value.

Script blocking

NoScript is an extension that allow blocking scripts execution per default, and to build a white list of allowed domains.

1. Install and activate the extension.
2. Fetch your fingerprint, how is it when script execution is blocked ?
3. Do some attributes still have a small anonymity set ?
4. Revert your changes by deactivating the extension.

Bonus - Manual fingerprint edition

You can spoof your whole fingerprint using Burp Suite, which is a proxy that will allow you to intercept and edit packets manually. We will use it to modify our fingerprints during their transfer.

Configuration

1. Install the Community Edition of the Burp Suite tool.
2. Launch it, and open a temporary project in default mode.
3. Go to the `Proxy` panel, then the `Options` subpanel.

4. Into `Intercept Client Requests` section, click `Add` and configure the following rule, it will only catch the packet containing the fingerprint :
    - `Boolean operator` : `And`
    - `Match type` : `Domain name`
    - `Match relationship` : `Matches`
    - `Match condition` : `results`
5. On your browser, open the `Preferences` window.
6. Scroll to the bottom of the page, find the `Network Settings` section and click on `Settings...` .
7. Select `Manual proxy configuration` , and configure the proxy as following :

- `HTTP Proxy` : `127.0.0.1`
- `Port` : `8080`
- Check `Use this proxy server for all protocols`

1. Validate these settings. *From now on, each request will be intercepted by the tool, and you will be able to edit, forward or drop them.*

Fingerprint edition

Before doing any manipulation from here, think how you will edit your fingerprint, do not hesitate to cooperate !

1. Go to the `Intercept` subpanel. *Here, you will see the request containing the fingerprint that is intercepted by the proxy.*
2. Fetch your fingerprint. *You should see a message saying that the certificate is invalid, allow an exception.*
3. Edit your fingerprint as you want, and look at the result afterward.

Andriamilanto Nampoina - tompoariniaina.andriamilanto@irisa.fr

12/13/2019