4.1 Summary [EHN18] "I never signed up for this! Privacy implications of email tracking"

E-Mails first used for only sending text-messages now evolved to be a subset of HTML which allow embedded images and stylesheet that are downloaded in order to be able to be viewed by the user. These requests are usually mad via third-party cookies with which a linking to web profiles is made possible. Additionally the email address itself is most often leaked to these third-party URLs. This can also happen when clicking on a link within an email because the request will contain user credentials which can be gathered by the website and linked to other already gathered information of the user.
In the here referred paper's study in 85% of all considered emails contained some form third-party content, and 70% contained some sort of tracking mechanisms which are listed on popular tracking-protection lists. Furthermore when simulating a normal user behaviour in an email client 29% of the emails leaked the user's email and 19% of senders sent at least an email with such a leak embedded within it. Based on the used heuristics it was concluded that at least 62% of the leaks were intentional and that with common tracking protection applications 87% of the leaks could be prevented. Furthermore it was conducted that the email views though not supporting Javascript are dynamic and each embedded resource in an email can return different responses eacht time it is viewed; it can even redirect to different third parties. But for the majority of the emails when opening them a second time only fewer third parties are loaded than when opening it the first time.
When adding blocking extensions like uBlock Origins, Privacy Badger or Ghostery in order to block tracking requests the occurances of email adress leaking were cut in half and also the number of senders which leak the email address is greatly reduced. However, most of the plaintext and email hashes leaks still occur.
Another way emails were leaking email adresses is via embedded links. Becuase these links typically open in a web browser which supports Javascript and advanced HTML features it is more prone to privacy leaks. In total these mechanisms are much less frequently used than the one discussed before, because it requires the direct embedding of the address in the original email body and needs to be manually clicked whereas the tracking mechanisms embedded in the email work on their own.
There are different ways to defend against these several kinds of privacy "attacks":
One way is content proxying with which embedded content is being proxied in order to not needing the mail user agent to make any requests to third parties.
Another option is HTML filtering which modifies the content of HTML in order to mitigate tracking. The problem with this defense system is that it can interfere with some email authentication methods like DKIM, but this can be mitigated by authenticating after the signature was verified.
Additionally there are cookie blocking, referrer blocking, and request blocking as defense systems.

4.2 AmIUnique

When opening the website in the TOR browser the particular browser fingerprint could not be identified and therefore was not traceable ;).
When using the chrome browser the browser fingerprint was unique. After adding the browser extensions uBlock, Ghostery, HTTPs Everywhere, AdBlock Plus, Disconnect, and Privacy Badger and additionally disabled all cookies the browser could not be uniquely identified anymore.

Bibliography

[EHN18] ENGLEHARDT, Steven ; HAN, Jeffrey ; NARAYANAN, Arvind: I never signed up for this! Privacy implications of email tracking. In: *Proceedings on Privacy Enhancing Technologies* 2018 (2018), Nr. 1, 109–126. `http://dx.doi.org/doi:10.1515/popets-2018-0006`. – DOI doi:10.1515/popets–2018–0006