Insecure private network requests: enterprise policies

Visibility: public

Author: titouan@chromium.org
Reviewers: clamy@chromium.org, bheenan@chromium.org
Status: **published**
Last modified: June 2021

Objective

Design Chrome enterprise policies allowing administrators to work around upcoming restrictions on insecure public websites fetching private network resources.

Background

In Chrome M93, we will be preventing non-securely delivered web pages from fetching resources from a user's private network. This is a small first step towards Private Network Access, designed in more detail in this design doc.

The broad idea is to prevent http://example.org from making arbitrary requests to a user's NAS or smart toothbrush, as the insecure web page's contents could be arbitrarily tampered with by a person-in-the-middle attacker.

We expect that some existing legitimate use cases depend on this flow, especially in enterprise contexts where network topology can be complex and internal web applications common, plus a common attitude that web traffic doesn't have to be encrypted when on an intranet behind a firewall. In order to prevent the new release from breaking such web pages, we will provide enterprise policies for administrators to selectively disable this feature.

Proposal

This setup is mostly cribbed from SameSite's policies (allowlist, big red button), as suggested by bheenan@. The main difference is that we apply the allowlist per origin instead of per domain. We define two policies:

- InsecurePrivateNetworkRequestsAllowed
    - Type: boolean

    - Values:
        - Unset = default, controlled by field trials
        - true = Allow private network requests on all insecure websites
        - false = Block insecure private network requests on all websites (as long as the feature is enabled, otherwise this settings does nothing)
- InsecurePrivateNetworkRequestsAllowedForUrls
    - Type: list of strings
    - Values:
        - Origin patterns, e.g. “https://www.example.com” or “[*.]example.com”
    - Allows private network requests from insecure websites belonging to an origin that matches any of these entries

These two policies are part of the same atomic group, just like the SameSite policies.

The goal is to support these policies on all platforms, as they affect behavior of the content layer only - AFAIU there is no additional cost to supporting them everywhere.

Alternatives considered

We could define an allowlist of *internal* websites that can be fetched by any public insecure website instead. This would probably be strictly worse in terms of security, as it would open up listed websites to e.g. http://evil.com.

We could further restrict each public website’s ability to load internal resources by specifying a pattern to match internal resources. For example: “foo.com is allowed to fetch bar.intranet”. It is not clear the additional effort to implement this would be worth the security gains. This is all the more true given that we want to eventually implement Private Network Access, which provides a much richer way for websites to declare their availability to externally-initiated requests.