ArpFilterProposal

ArpFilter before the profile servlet - support for other authentication modules

ArpFilter and ArpViewer works great, but there is one big problem with ArpFilter: it only supports REMOTE_USER -based authentication. Shibboleth2 IdP comes with username and password module, which can be extended to use with any JAAS-compliant Login module. Unfortunately, current ArpFilter design can not work with this module.

So I made some research to find out how to bring ArpFilter and Shibboleth IdP's internal authentication modules together. My motivation was to support the shipped UserPassword authentication and many of the features that Shibboleth IdP has (forceAuthn, isPassive).

I found out that ArpFilter only depends on Shibboleth's LoginContext. This LoginContext is created by the profile handler code and interpreted by the authentication engine (and authentication modules) - then, after authentication succeeds, the profile handler processes the LoginContext and issues the response to the SP that requested it.

So my idea is simple: why ArpFilter is put before the authentication servlets instead of the profile handler servlet?

I got ArpFilter work before the profile servlet, but not quite sure whether my solution works in all use cases where it should do. I have tested it with SAML2 requests and UserPassword authentication and it seemed to work. Even the PreviousSession authentication handler did with no additional need of PreviousSessionServlet.

Of course I made some modifications to the original ArpFilter code, but not too much. Basically, it just looks for LoginContext and makes sure the profile servlet gets the LoginContext, even if ArpFilter is called.

The code logic is the following:

- Ensure that the request is made to the profile servlet.
- Try to get LoginContext from session.

    - If LoginContext is found in the session, transfer it back to the request scope and remove it from the session.
- Try to get LoginContext from request scope.
    - If no LoginContext found, proceed to the profile servlet and exit.
    - Else process the request as usual, and find username in the IdP session.
- In the case when ArpFilter decides to hand over the control to the ArpViewer application, save the LoginContext back to Session.

I needed one more little modification to web.xml: remove filters from /Authn/ servlets and put the ArpFilter in front of the ProfileHandlerServlet (and include the 'forward' dispatcher here, because the profile handler servlet gets the second request from the authentication engine with servlet forward - when the authentication is succeeded).

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:33 CEST
cziernorbert frissítette 2026-04-14 13:22:33 CEST