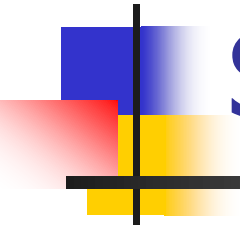
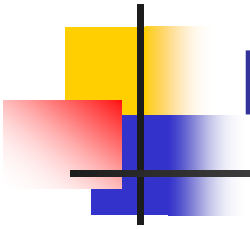


Security modules for Apache

Daniel Kouřil, Matej Prišťák

AFS & Kerberos Best Practices Worshop 2009



mod_auth_kerb - 5.4

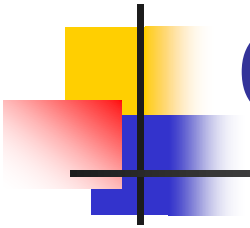
- released in Dec 2008
- Several patches from the community
  - ANY for key selection, …
- Support for aname_to_lname()
  - Stripping realm name
- Optimization and bug fixes
  - Build doesn‘t require GNU make

mod_auth_kerb – CVS

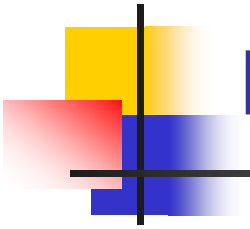
- Basic provider for Kerberos
  - Requires Apache 2.2
  - Multiple mechanisms for password verification

```
AuthType Basic
AuthName "Basic authN"
AuthBasicProvider file kerberos
AuthUserFile /etc/apache2/htpasswd
KrbAuthRealms EXAMPLE.ORG
Require valid-user
```

General authN provider

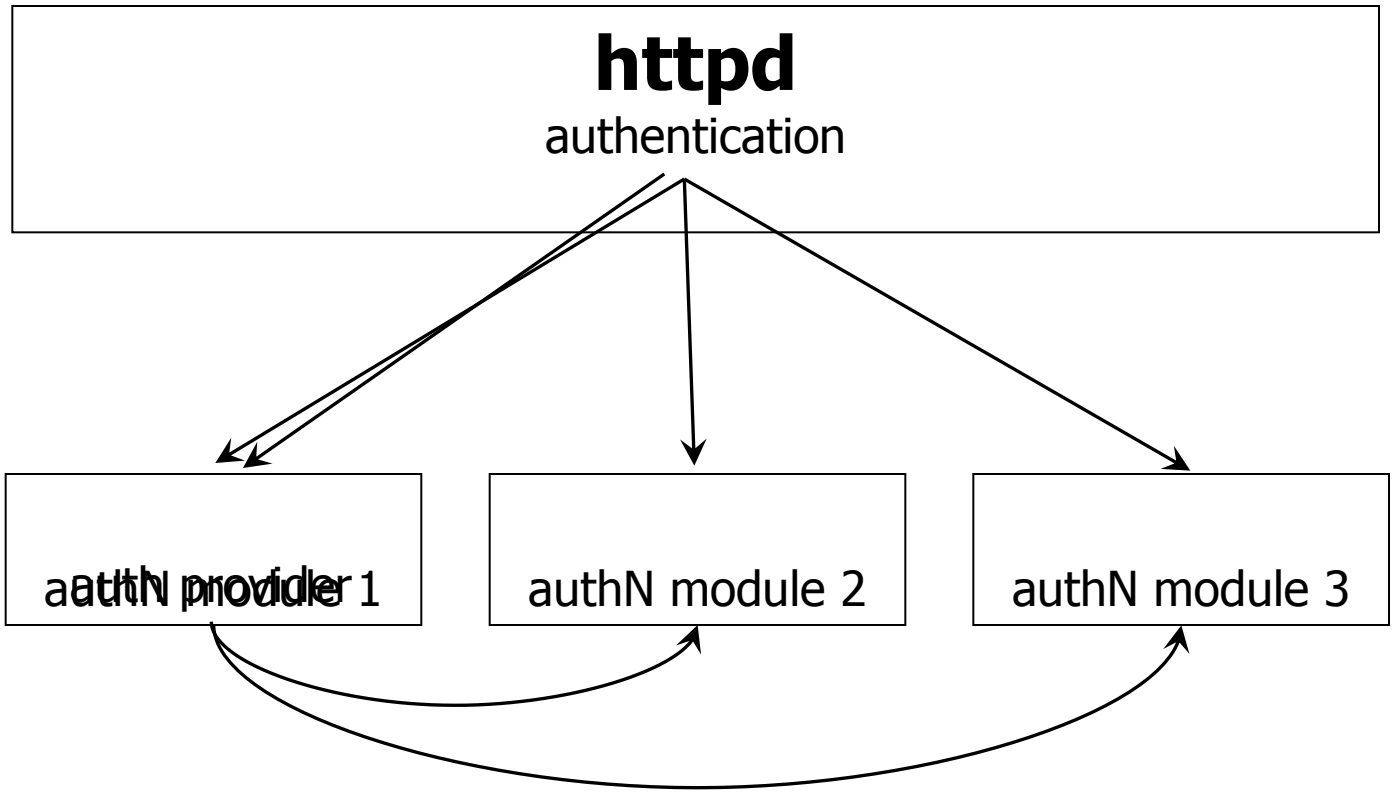


- Basic/Digest/… providers support only a single authN type
  - Users use X.509, Negotiate, local passwords and Kerberos passwords, …
  - Multiple authN types can‘t be specified
- General provider
  - support more authN mechanisms
  - PoC implementation available
    - meta.cesnet.cz/soubory/mod_auth_provider.tar.gz
  - Extended AuthType directive



mod_auth_provider

- New layer between Apache and modules API
  - Existing modules are plugged in
  - Implemented as authN module
  - forced to be invoked first in the chain
    - Other modules get never called
- No adaptations of existing modules needed

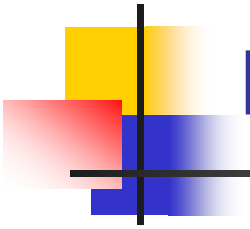

httpd
authentication
authN module 1
authN module 2
authN module 3

Username mappings

- Multiple identifiers of the same user

```
/DC=cz/DC=cesnet-ca/O=Masaryk University/CN=Daniel Kouril
CN=Daniel Kouril,O=Masaryk University,DC=cesnet-ca,DC=cz
kouril@ICS.MUNI.CZ, kouril@META
1388@muni.cz
```

- Difficult management of authZ policies
- Difficult maintanance of applications
  - Adding new authN methods requires changes in application code



mod_map_user

- Rule-based rewritting of usernames
  - PoC implemented and available
    - CVS module next to mod_auth_kerb
- Implements the authZ API of Apache
  - Called after authN as the first authZ module
- Two mapping schemas:
  - MapUsernameFile <file>
    - File consists of lines <orig_name> <new_name>
  - MapUsernameRule [<auth_type>:]<RE> <result>
    - Kerberos:(.*)@(.*) "$1"

Putting all together

```
AuthTy
SSLVer
SSLOpt
AuthBa
KrbMethodK5
MapUsernam                /ap
MapUsernar                Kerbero
MapUserna                 Rule Basic:(                                    RG"
require valid-user
```

kouril@EXAMPLE.ORG
kouril
/DC=cz/DC=cesnet-ca/O=Masaryk University/CN=Daniel Kouril

Or:

```
AuthLDAPURL ldap://ldap.example.org/ou=People,dc=EXAMPLE,dc=ORG?dn?one
require ldap-attribute authorized=yes
```

kouril:$apr1$...Qt9v...$EPr7.g0.CuS99ehguitCo.
/DC=cz/DC=..../CN=Daniel Kouril:xxj31ZMTZzkVA