SSSD: FROM AN LDAP CLIENT TO SYSTEM SECURITY SERVICES DEAMON

ABOUT ME AND THE TALK

- I'm a developer working for Red Hat, mostly on SSSD
- Twitter: @JakubHrozek
- Github: https://github.com/jhrozek/fosdem2018
- This talk is about SSSD, but (hopefully) not about the known parts

TALK TOPICS

- Several topics, the talk might be fast
  - please get in touch for more details about any topic
- SSSD APIs
- Local user handling
- Smart card management (for local users)
- Kerberos ticket management

SSSD APIS

TALKING TO SSSD FROM AN APP

SSSD API USE-CASES

- Many applications implement some sort of an "LDAP driver" or an "LDAP connector"
  - typically app-specific code, not reusable
- The job is not as easy as it might sound
  - Server discovery, affinity, fail over, caching, different schemas
  - SSSD is a "domain expert", let's leverage it!

HOW DOES ONE TALK TO SSSD

- API vs. plugin
- SSSD already provided several *plugins* for system APIs
  - NSS - getent passwd $user -> getpwnam(3) -> _nss_sss_getpwnam
  - Nontrivial to call directly, only through the system API
  - Somewhat inflexible, e.g. getpwnam(3) can only return "struct passwd"

TALKING TO SSSD DIRECTLY

- D-Bus API
  - Pros: many language bindings, type-safe, signals (notifications), introspection
  - Cons: Requires a system bus, some language bindings not that great
  - Currently used by several applications like ManageIQ, Keycloak, mod_lookup_identity, ...
- Would some other API be more appealing to a project?
  - REST perhaps?
  - ldapi:// ?

DEMO TIME

- D-Bus API example compared to raw Python
- Keep in mind the raw Python script doesn't to caching, failover, service discovery, ...
- Two D-Bus examples
  - https://github.com/jhrozek/fosdem2018/tree/master/dbus-api
  - The OO one is more verbose but more flexible as well
    - all objects are represented with a path regardless of how was the object found
    - signals (notifications)

MANAGING LOCAL USERS

SSSD AND /ETC/{PASSWD,GROUP}

MOTIVATION

- Faster NSS API access without nscd
- Leverage the same APIs for local and remote users
- Additional attributes
- Smart cards for local users
  - separate section later

CURRENT STATUS

- Caching enabled in Fedora since F-26
  - https://fedoraproject.org/wiki/Changes/SSSDCacheForLocalUsers
  - sssd is running by default
  - /etc/passwd and group are mirrored into sssd on-disk cache
  - any request triggers putting the user or group entry into mmap-ed cache
  - without nscd or sssd, a request would trigger opening and parsing the files
- Pros: Interoperates easily with other SSSD domains, unlike nscd
- Cons: SSSD is "fatter" than nscd, requires modifications to nsswitch.conf
  - `passwd: sss files`
  - This doesn't require sssd to be running, though!

FUTURE DEVELOPMENT

- Improve the smart card integration for local users
  - More on this later in this presentation..
- Enable extending the SSSD database with extra attributes
  - Currently the 'sss_override' tool can be used to add certs, but there's no general API
- Extend the D-Bus API to enable user database modifications
  - probably backed by libuser?
- Implement the https://www.freedesktop.org/wiki/Software/AccountsService/ API to get a consistent API for local and remote users
- Hopefully will happen this year...

SMART CARDS WITH SSSD

FOR LOCAL AND REMOTE USERS

DISCLAIMER

- I'm not a Smart Cards expert
- The previous Jakub is
  - https://fosdem.org/2018/schedule/event/smartcards_in_linux/
  - https://www.youtube.com/watch?v=x2mpba45UVc
- Not even expert in this part of SSSD
- Nonetheless, let's illustrate the state

CURRENT STATE

- Traditionally, pam_pkcs11 had been used
  - lot of features, stable
  - also dead upstream..
  - doesn't build against recent OpenSSL, was removed from Fedora
- SSSD in the meantime gained support primarily for remote users
  - FreeIPA/IDM + AD trusts is the main scenario
    - match or list user(s) against a certificate stored in the directory
    - "local" authentication with the help of the keys on the smart card or Kerberos PKINIT
  - ~~Usable~~Functional for local users as well already

SMART CARDS FOR LOCAL USERS

- Several manual configuration changes needed now
- SSSD must be serving users from local files
- Works with anything that implements the pkcs11 interface
  - the demo is using a Yubikey
- The user database must augmented with the certificate
- pam_sss, not pam_unix must be handling authentication
- Should work in a user-friendly manner in Fedora-29

DEMO TIME

- Smart card authentication with SSSD and a local user

SSSD-KCM

LET SSSD HANDLE YOUR KRB5 TICKETS

WHERE'S MY TICKET?

- Any successful Kerberos authentication yields a "ticket"
  - KDC initial authentication (kinit) -> TGT
  - service authentication -> service ticket
- A blob that must be stored in a *credential cache*
- Several options
  - FILE, DIR, KEYRING, **KCM** ...

KCM AND SSSD-KCM

- KCM is not our idea
- Comes from the Heimdal Kerberos distribution, circa 2005
- The credentials are handled by a daemon
  - All the other credential cache types are "passive"
  - The application (e.g. kinit) is a client, KCM daemon is a server
  - Client talks to the KCM server over a UNIX socket
- At the moment, Heimdal implements both server and client, MIT only the client
  - you can mix and match, though

KCM CCACHE BENEFITS

- Stateful
  - renewals, notifications, cleanup of expired caches or on logout ...
- Credentials are not written to disk
- Better suited for containers
  - UNIX socket can be selectively shared between containers or container and host
  - The KCM deamon is subject to namespacing (root in container vs. root on host)
  - Do people use Kerberos with containers, though?

SSSD-KCM

- SSSD-KCM is an implementation of the KCM server
  - reuses a lot of SSSD code, but doesn't need the rest of SSSD
  - systemctl enable sssd-kcm.socket should be enough
  - planning to use some private SSSD APIs for advanced features (notifications, ...)
- Default Kerberos cache in Fedora since F-27
  - some open bugs, though..
- Feature-wise equivalent to other ccache types, more improvements planned for F-29
  - renewals
  - notifications
  - ...and more

MORE RESOURCES

- SSSD upstream design page:
  - https://docs.pagure.org/SSSD.sssd/design_pages/kcm.html
- MIT documentation
  - http://k5wiki.kerberos.org/wiki/Projects/KCM_client

QUESTIONS?

THANK YOU FOR LISTENING!