Подходы к внедрению мандатного управления доступом на этапе проектирования механизмов межпроцессного взаимодействия ОС семейства Linux

Буренин Павел
(ФУМО ВО ИБ)

Межпроцессное взаимодействие D-Bus

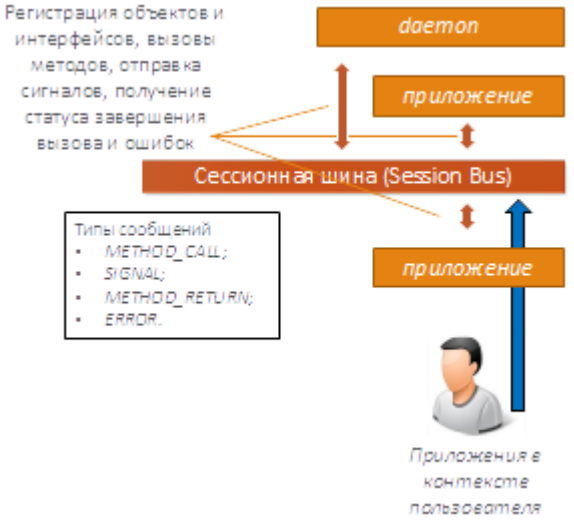
Элементы взаимодействия D-Bus

Шины: Session Bus, System Bus, Accessibility Bus.

Объекты на шинах и вызовы их методов: сервисы (services), пути (paths), интерфейсы (interfaces), методы (methods)

Отложенная активация сервисов

Системные обращения к D-Bus



Информационные потоки и управление объектами в системе D-Bus

- Взаимодействие сервисов и клиентов на различных уровнях конфиденциальности
- Формирование широковещательных сообщений и сигналов
- Доступ к сервисам для их перечисления
- Получение информации с использованием системных вызовов
- Формирование очередей владельцев сервисов

Построение систем управления доступом с использованием D-Bus

- Реализация управления доступом в самом механизме D-Bus для исключения необходимости контроля разработчиков сторонних сервисов
- Принятие решения о доставке сообщений на основании меток сообщения, источника и получателя
- Считывание и анализ привилегий взаимодействующих процессов
- Инициализация меток целостности и конфиденциальности при операции получения доступа «владения» для сервисов
- Применение таблиц контекстов сервисов, содержащих метки целостности и конфиденциальности, с возможностью конфигурации по файлам настроек
- Контроль широковещательных сообщений и сигналов
- Контроль обращений к сервисам
- Контроль «системных вызовов системы D-Bus»

Мандатное управление доступом при системных вызовах D-Bus

- **ListQueuedOwners**

Текущий владелец Уровень 0, следующий – Уровень 1

```
user@astra:/test$ dbus-send --system --dest=org.freedesktop.DBus --type=method_call --print-
reply /org/freedesktop/DBus org.freedesktop.DBus.ListQueuedOwners string:"org.share.server"
method return sender=org.freedesktop.DBus -> dest=:1.134 reply_serial=2
   array [
      string ":1.130"
      string ":1.131"
   ]
```

Запрос с уровня 1

```
user@astra:/test$ dbus-send --system --dest=org.freedesktop.DBus --type=method_call --print-
reply /org/freedesktop/DBus org.freedesktop.DBus.ListQueuedOwners string:"org.share.server"
method return sender=org.freedesktop.DBus -> dest=:1.135 reply_serial=2
   array [
      string ":1.130"
   ]
```

Запрос с уровня 0

:1.130 уникальный идентификатор соединения процесса с меткой 0:0:0:0 (Уровень 0)

:1.131 уникальный идентификатор соединения процесса с меткой 1:0:0:0 (Уровень 1)

Мандатное управление доступом при системных вызовах D-Bus

```
---------------------------------------- org.share.server : GetConnectionUnixUser ------------------
Error org.freedesktop.DBus.Error.AccessDenied: Could not get UID of name 'org.share.server': access failed
---------------------------------------- org.share.server : GetConnectionUnixProcessID -------------
Error org.freedesktop.DBus.Error.AccessDenied: Could not get PID of name 'org.share.server': access failed
---------------------------------------- org.share.server : GetNameOwner ---------------------------
Error org.freedesktop.DBus.Error.AccessDenied: Could not determine unique name for 'org.share.server' access failed
```

Запрос GetConnectionUnixUser, GetConnectionUnixProcessID/GetNameOwner с уровня 0

```
---------------------------------------- org.share.server : GetConnectionUnixUser ------------------
method return sender=org.freedesktop.DBus -> dest=:1.93 reply_serial=2
   uint32 1000
---------------------------------------- org.share.server : GetConnectionUnixProcessID -------------
method return sender=org.freedesktop.DBus -> dest=:1.94 reply_serial=2
   uint32 8129
---------------------------------------- org.share.server : GetNameOwner ---------------------------
method return sender=org.freedesktop.DBus -> dest=:1.95 reply_serial=2
   string ":1.23"
```

Запрос GetConnectionUnixUser, GetConnectionUnixProcessID/GetNameOwner с уровня 1

Спасибо за внимание.

Вопросы?