DevFest Perros-Guirec 2021

IOT BZH

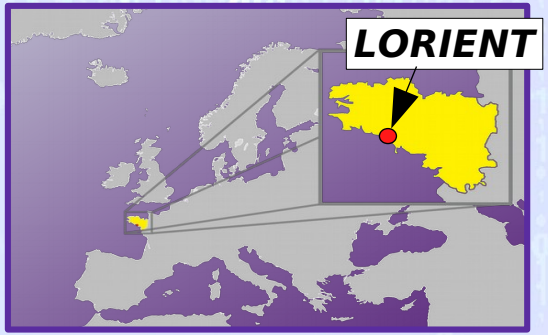
Clément Bénier

Fulup Ar Foll

Automatisation des modules de sécurité Linux en intégration continue

About us

- 30 engineers dedicated to embedded Linux
- 6 nationalities, 20% women in engineering
- Worldwide recognition within open source community
- 1st AGL technical contributor past 5 years



Release of redpesk Arz 1.0

redpesk® Arz 1.0 includes the following key features :

- A new application framework AFB-V4 engine compatible with AGL-V3 up to 10 times faster
- A new security model that can understand Smack but also an early access version for SELinux
- +2 500 pre-built ready-to-use binary packages

But also many others as:

- Cross-compilation for X86 & ARM architectures
- SDK enabling fast native iteration cycles for developers
- Automatic testing facility for both real & virtual environments
- Extended QA through scanning tools
- Release management solution
- Reporting interface
- Reference implementation for Over-the-Air updates
- Core optional platform services (health monitoring, identity management etc)

https://redpesk.bzh/welcome/news/arz1.0

Automatisation des modules de sécurité Linux en intégration continue

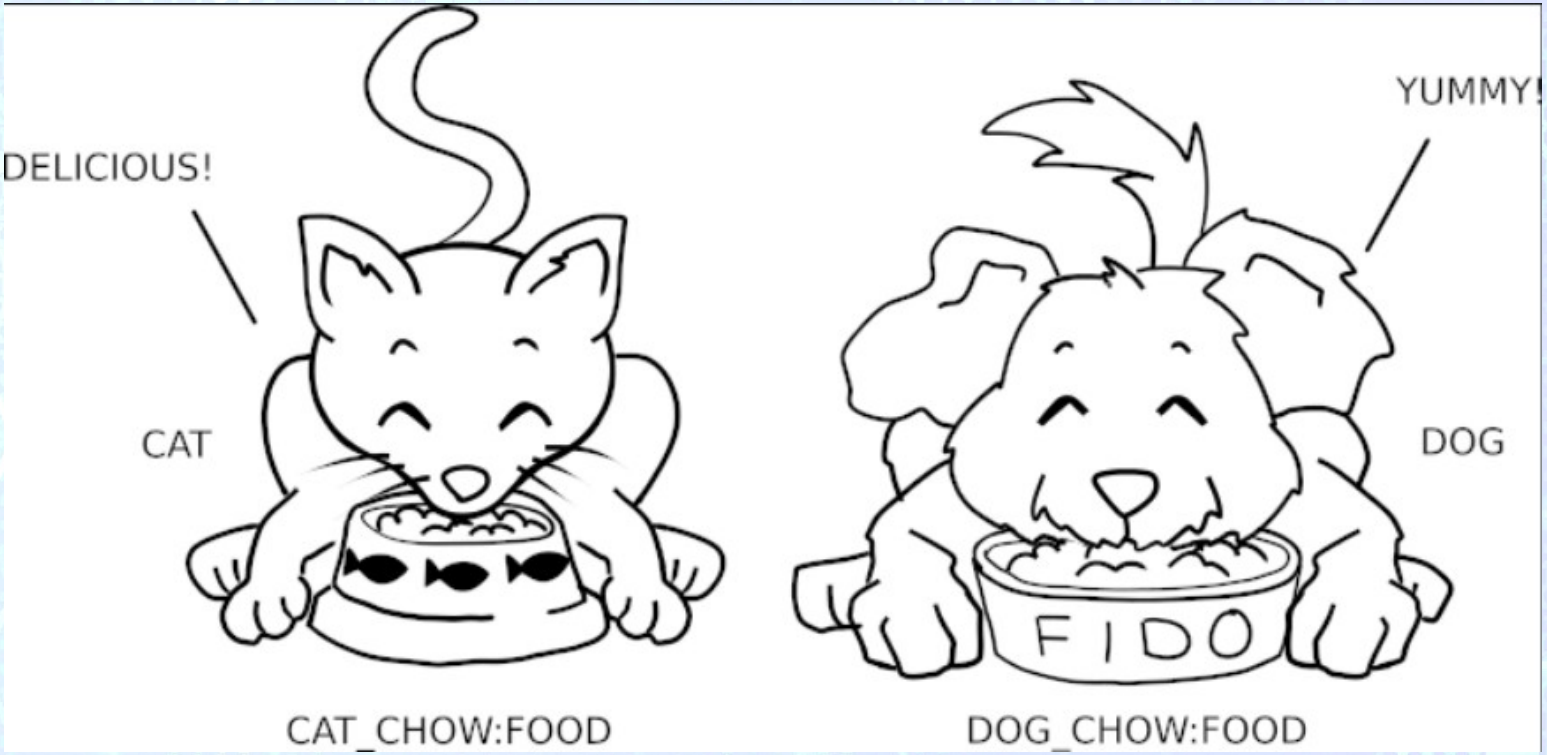
1) Problème: Isoler nos ressources
2) Présentation des Mandatory Acces Control
    1) Smack
    2) SELinux
3) Automatisation de la politique de securité dans redpesk
4) Aller plus loin
    1) Identité (secure-gate)
    2) Conteneur léger: redpak

1) Problème: Isoler nos ressources

- 0Day
- Shell sur une machine
- Limiter un processus à ce dont il a besoin uniquement:
  - ✘ Acces à d'autres fichiers
  - ✘ Acces aux processus
- Demo server hack

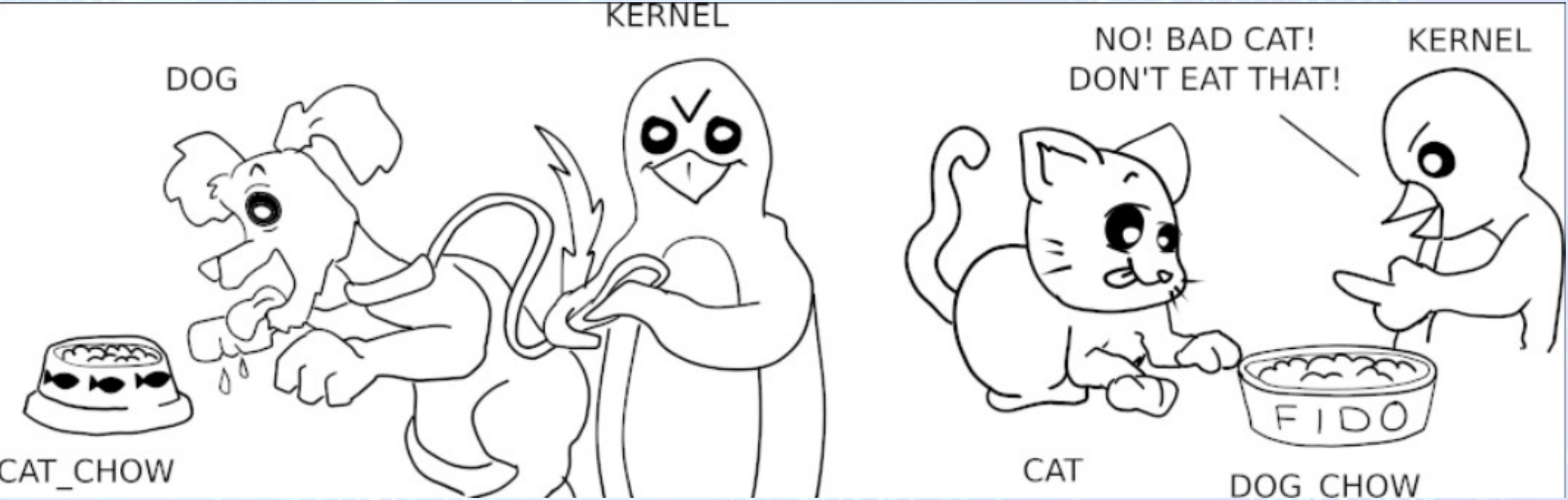
```
systemctl cat serverhack
...
[Service]
User=rp-owner
Type=simple
WorkingDirectory=/home/1001/devfest
ExecStart=/opt/bin/serverhack.py
```

1) Chiens et Chats



The selinux coloring book: "It's raining cats and dogs!"
https://people.redhat.com/duffy/selinux/selinux-coloring-book_A4-Stapled.pdf

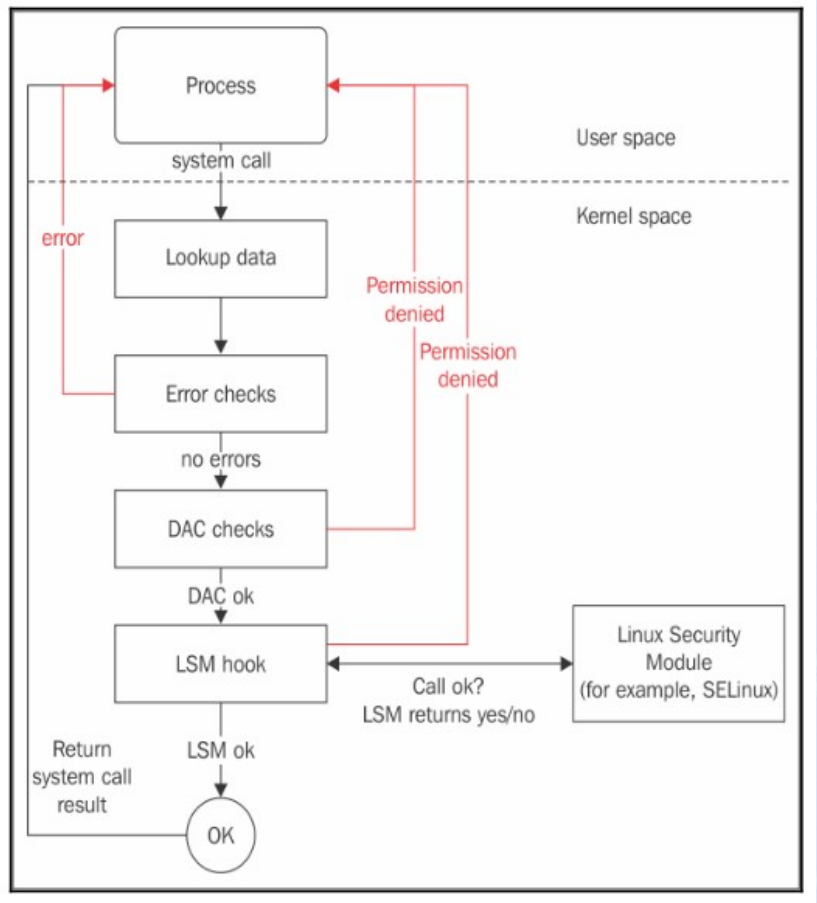
1) Chiens et Chats



The selinux coloring book: "It's raining cats and dogs!"
https://people.redhat.com/duffy/selinux/selinux-coloring-book_A4-Stapled.pdf

2) LSM

- Kernel module
- Dac extension
- Processus, fichiers, utilisateurs labelisés
- Charge des modèles de sécurité (SMACK, SELINUX,...)

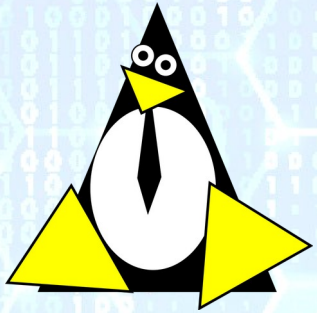


2) MANDATORY ACCESS CONTROL

✔ Protection contre les 0DAY
✔ Politique de sécurité gérée par les administrateurs
✔ Renforce la confidentialité et l'intégrité de données

✗ Antivirus
✗ Remplacement de mots de passe, pare-feux, …
✗ Solution tout-en-un

2) Examples de MAC

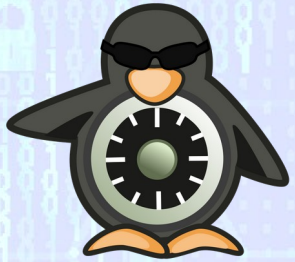


SMACK
(Tizen, AGL)

- Très simple
- Dynamique
- Dédié à l'embarqué

APPARMOR
(Ubuntu, debian)

- Simple
- Des regles pour certaines applicattions

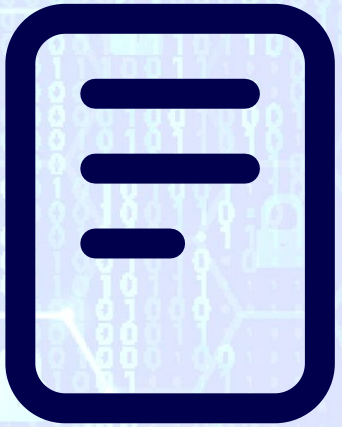


SELINUX
(Redhat, Android)

- Complexe
- Règles pour presque toutes les applications

2.1) Smack: Labels sur les fichiers

- Type de fichier
- Taille
- Droits d’acces (DAC)
- UID,GIG
- …
- **Attributs étendus**



```
ls -Z toto

unconfined_u:object_r:user_home_t:s0 toto                    # SELINUX
System toto                                                  # SMACK
```

2.1) Smack: Labels sur les processus

- Type de processus
- Droits d'acces (DAC)
- UID,GIG
- ...
- **Fichier current**

```
ps -Z $$
LABEL                                                PID COMMAND
System                                              1061 bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1041 bash
```

2.1) Règles Smack

Label_sujet Label_object Permissions

- r: read
- w: write
- x: execute
- a: append

App:helloworld-binding User:App-Shared rwx
App:helloworld-binding System wx

/etc/smack/accesses.d/

2.1) Demo Smack

```
cat /etc/smack/accesses.d/serverhack.smack
ServerHack System wx
ServerHack System:Shared rx
System ServerHack wrx
System Secret wrx
```

```
systemctl cat serverhack-smack
...
[Service]
User=rp-owner
Type=simple
WorkingDirectory=/home/1001/devfest
SmackProcessLabel=ServerHack
ExecStart=/opt/bin/serverhack.py
```

2.2) Label Selinux

Utilisateur -> Role -> Type Sensibilité

system_u:object_r:**helloworld_binding_exec_t**:s0
system_u:object_r:**helloworld_binding_conf_t**:s0

2.2) MODULES

- Module .pp chargé dans la politique SELinux
- Définit par 3 fichiers:
  - *.te*: règles
  - *.fc*: labels fichiers
  - *.if*: interfaçage

```
semodule -i module.pp
```

Règles SELinux

allow serverhack_t serverhack_t:tcp_socket {listen read}

Verbe
- Allow
- Dontaudit
- Auditallow
- neverallow

Type du sujet

Type et classe de l'objet

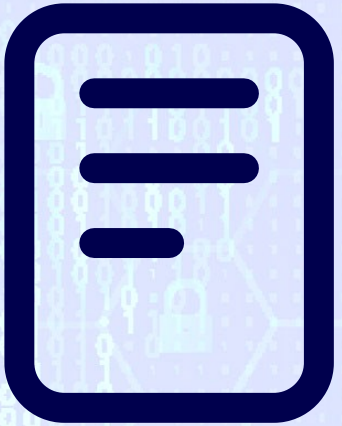
Autorisations

2.2) Règles SELinux: Fichier .te

```
policy_module(serverhack,1.0.0)

type serverhack_t;
type serverhack_exec_t;
init_daemon_domain(serverhack_t, serverhack_exec_t);

type serverhack_data_t;

corecmd_exec_bin(serverhack_t);
allow serverhack_t self:tcp_socket { bind create getattr };
allow serverhack_t self:tcp_socket create_stream_socket_perms;
...
```

Labeliser fichiers

- .fc: file context



/usr/share/app(/.*)? gen_context(system_u:object_r:**app_usr_t**,s0)

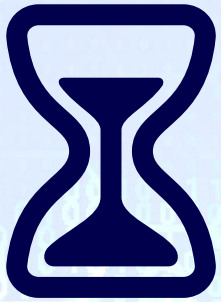
```
restorecon -R /usr/share/app
```

2.2) Fichier .fc

```
/opt/bin/serverhack.py gen_context(system_u:object_r:serverhack_exec_t,s0)
/home/1001/devfest/pas_secret gen_context(system_u:object_r:serverhack_data_t,s0)
/home/1001/devfest/secret gen_context(system_u:object_r:secret_data_t,s0)
```

2.2) Demo serverhack selinux

```
systemctl cat serverhack-selinux
...
[Service]
User=rp-owner
Type=simple
WorkingDirectory=/home/1001/devfest
SELinuxContext=system_u:system_r:serverhack_t:s0

ExecStart=/opt/bin/serverhack.py
```



Performance

Action	Installation (ms)	Supression (s)	Fichier (ms)	P (ms)
Désactivé			7614	198666
Smack	3.334	2.116	7896	204314
Selinux	20.452	9.729	8014	209122
Smack/Désactivé			3.5%	2.8%
Selinux/Smack	511%	359%	1%	2%

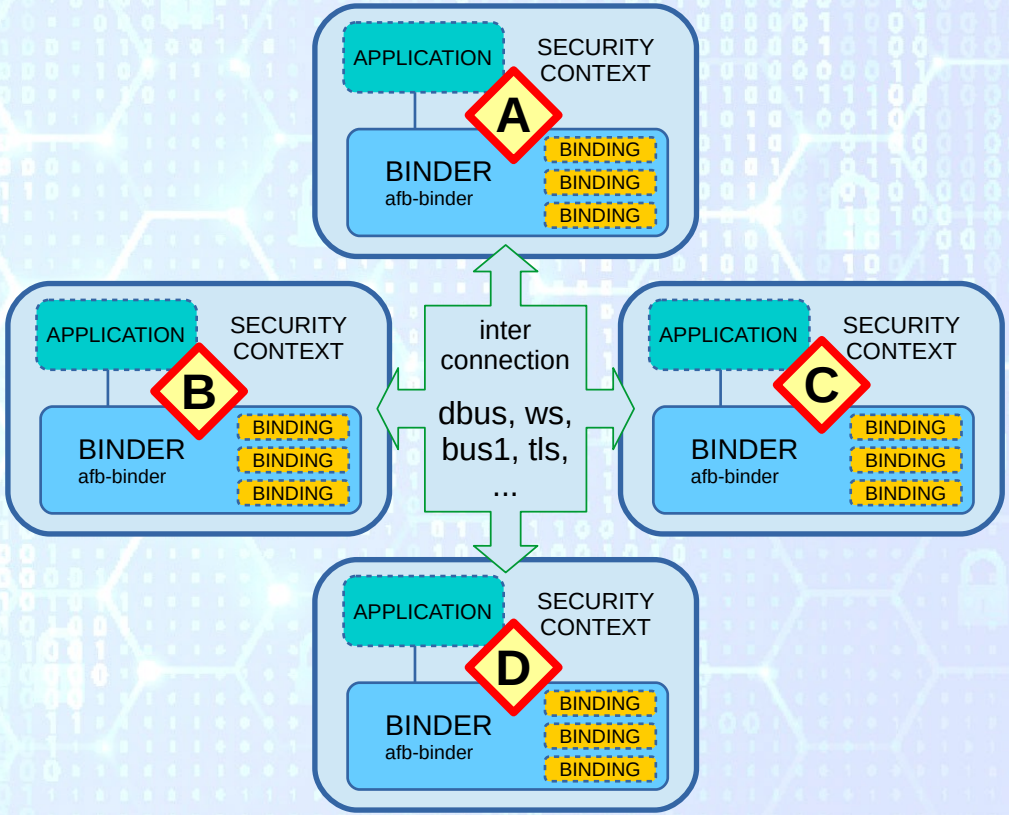
3) Faciliter la politique de sécurité pour les développeurs

- La partie système est déjà gérée
- Peut être complexe demande du temps des prérequis
- Les développeurs sont récalcitrants
- Isolations des applications
- Les managers sont contents

3) Redpesk

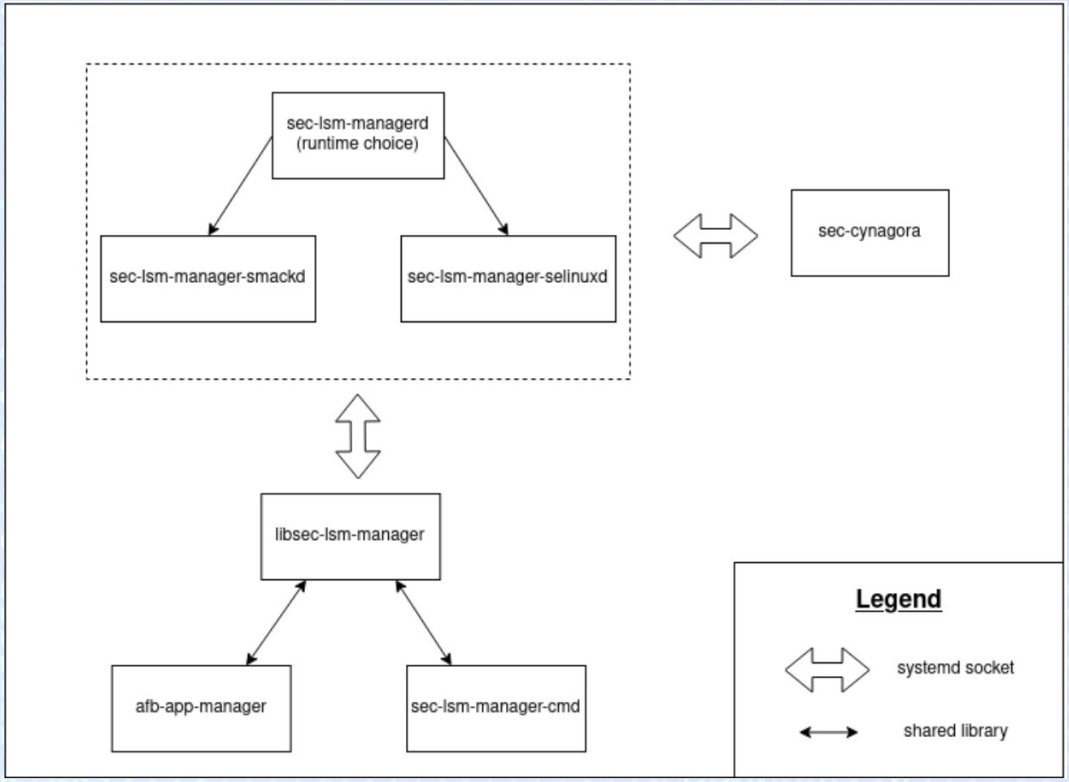
- RedpeskOS: Distro embarqué smack ou selinux
- Framework de securité
  - binders
  - sec-lsm-manager: interaction avec le modèle de sécurité et cynagora (Smack/SELinux)
  - Sec-cynagora: gestion des permissions entre bindings
  - ...
- Bindings (canbus, signal-composer, modbus, ble-sensor, ...)
  - Api: verbes/events

Framework de sécurité



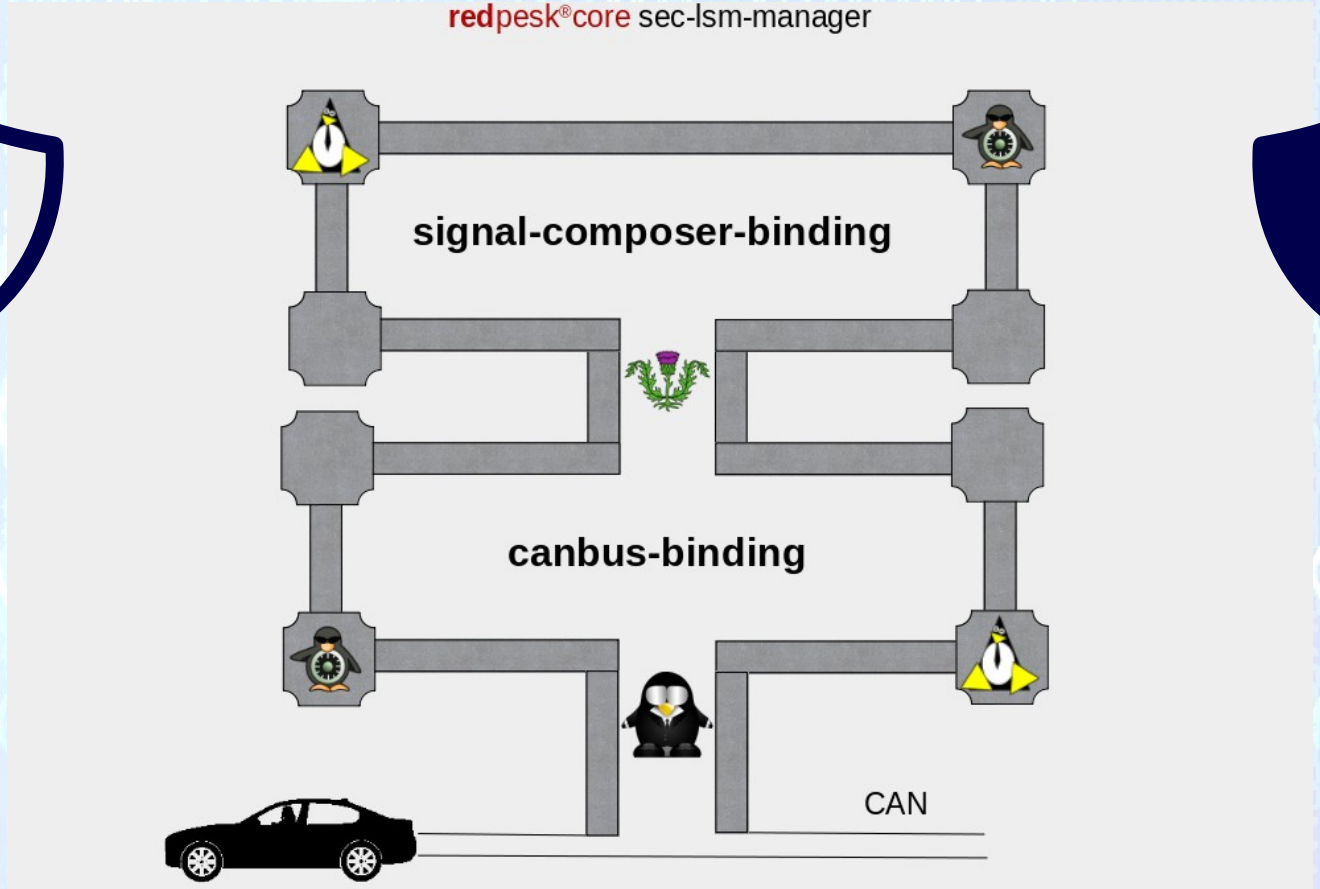
3) Sec-lsm-manager

- Création de politique de sécurité SMACK/SELinux
- Templates (mustach)
- Load into policy
  - Compile module (selinux)
  - Crée fichier de règles (smack)



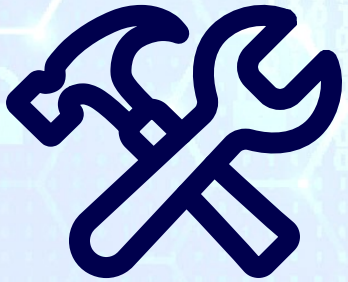
Arthur Guyader: Intégration de SELinux dans redpesk
https://iot.bzh/en/publications/44-2021/117-introduction-to-smack-and-selinux

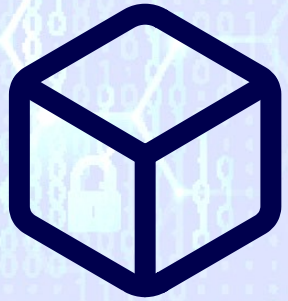
Bindings in redpesk



3) Packaging

- Rpm signés
- Plugin rpm appelle sec-lsm-manager
  - config.xml (ajout de règles de sécurité particulière)
  - Templates (règles, service systemd)
  - installation/desinstallation (ajout/retrait des règles)



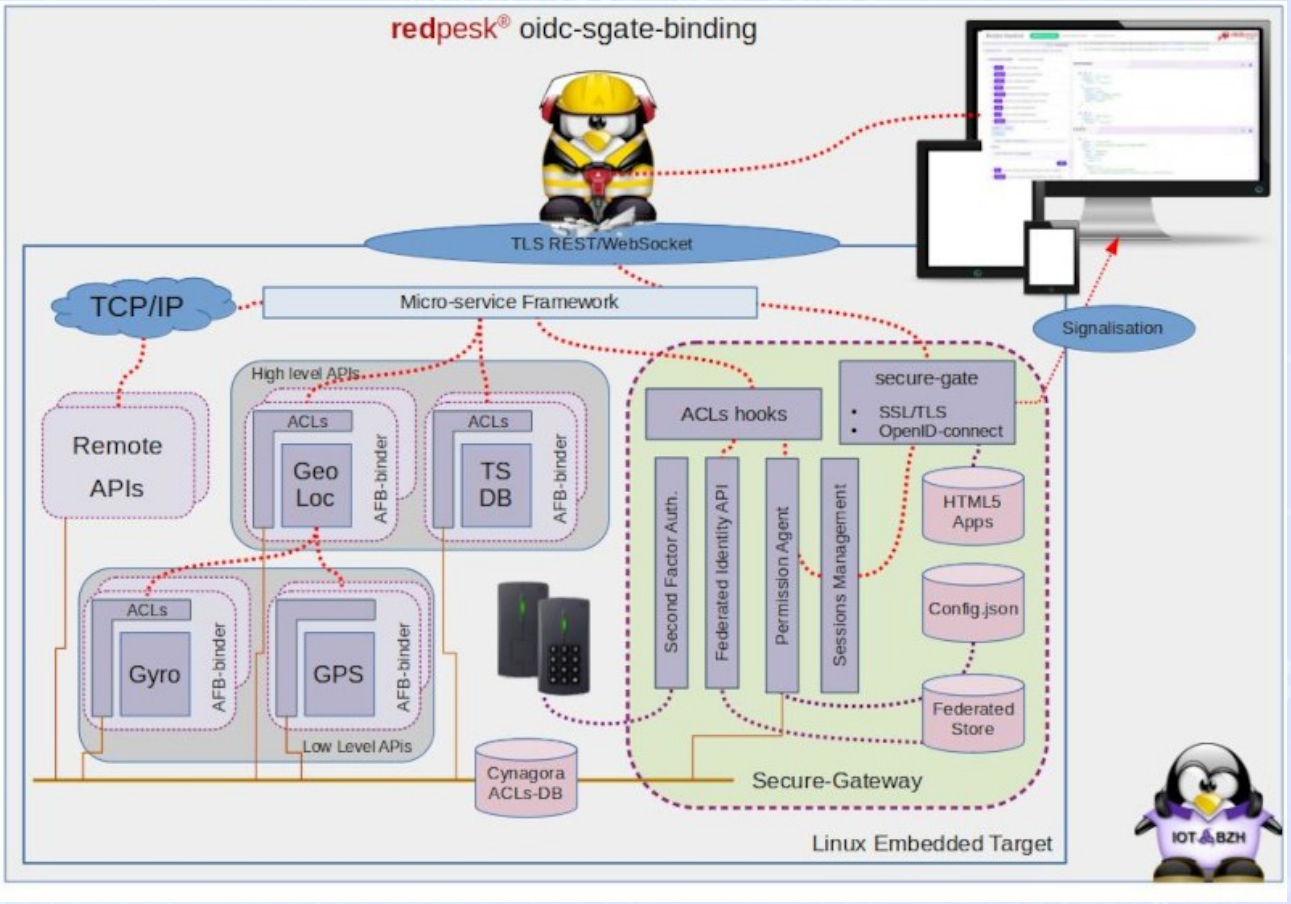


3) Demo canbus-binding

```
<?xml version="1.0" encoding="UTF-8"?>
<widget xmlns="http://www.w3.org/ns/widgets" id="canbus-binding" version="1.0">
     <name>canbus-binding</name>
     <content src="lib/afb-canbus-binding.so" type="application/vnd.agl.service"/>
     <description>Expose CAN bus  APIs through AGL Framework</description>

     <feature name="urn:AGL:widget:required-permission">
          <param name="urn:AGL:permission::partner:scope-platform" value="required" />
          <param name="urn:AGL:permission::partner:create-can-socket" value="required" />
          <param name="urn:AGL:permission::system:run-by-default" value="required" />
     </feature>

     <feature name="urn:AGL:widget:provided-api">
          <param name="canbus" value="ws" />
     </feature>

     <feature name="urn:AGL:widget:required-binding">
          <param name="lib/afb-canbus-binding.so" value="local" />
     </feature>
</widget>
```

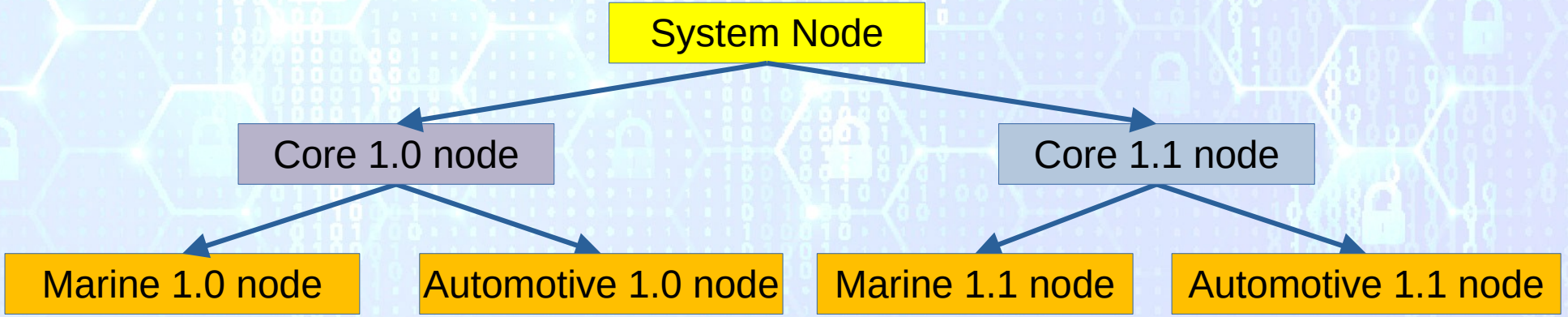
4.1) Pour aller plus loin: sec-gate

- Qui ?
- openID/nfc
- Extension binder
- Cynagora permissions
  - Ex: gps binding
    - Acces position tous les 300ms max



4.2) Pour aller plus loin: Redpak

- Unprivileged sandbox tool
  - Create namespaces: pid, uts, empty mnt(/ in tmpfs)
  - Seccomp (system calls filter)
  - PR_SET_NO_NEW_PRIVS to turn off setuid binaries
- Restricted access
- Unprivileged Users
- Configurable with yaml files
- Nodes

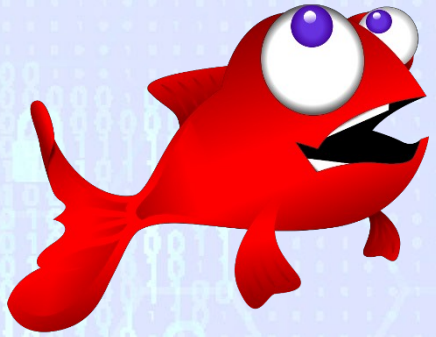


Q&A

Lorient Harbour, South Brittany, France

Links

- **redpesk®**
  - Website: https://redpesk.bzh/
  - Documentation: https://docs.redpesk.bzh/
  - Sources: https://github.com/redpesk/readme
- **IoT.bzh**
  - Website: https://iot.bzh/
  - Publications: https://iot.bzh/en/publications
  - Videos: https://vimeo.com/search?q=redpesk
- **Community Support**
  - Matrix.org: +redpesk:matrix.org



redpesk®