

## Writing secure HTML5 applications for automotive systems

## Table of contents

- *Introduction*
- *HTML5 application development*
  - *Modern development methods*
  - *Platform APIs as HTTP REST APIs*
- *Application framework platform design*
  - *Application Framework Manager*
  - *Application Framework Binders(s)*
- *Privilege isolation through SMACK and Cynara*
  - *SMACK labels, Cynara policies*
  - *Security for Application Framework Binder*



## What is an automotive system ?

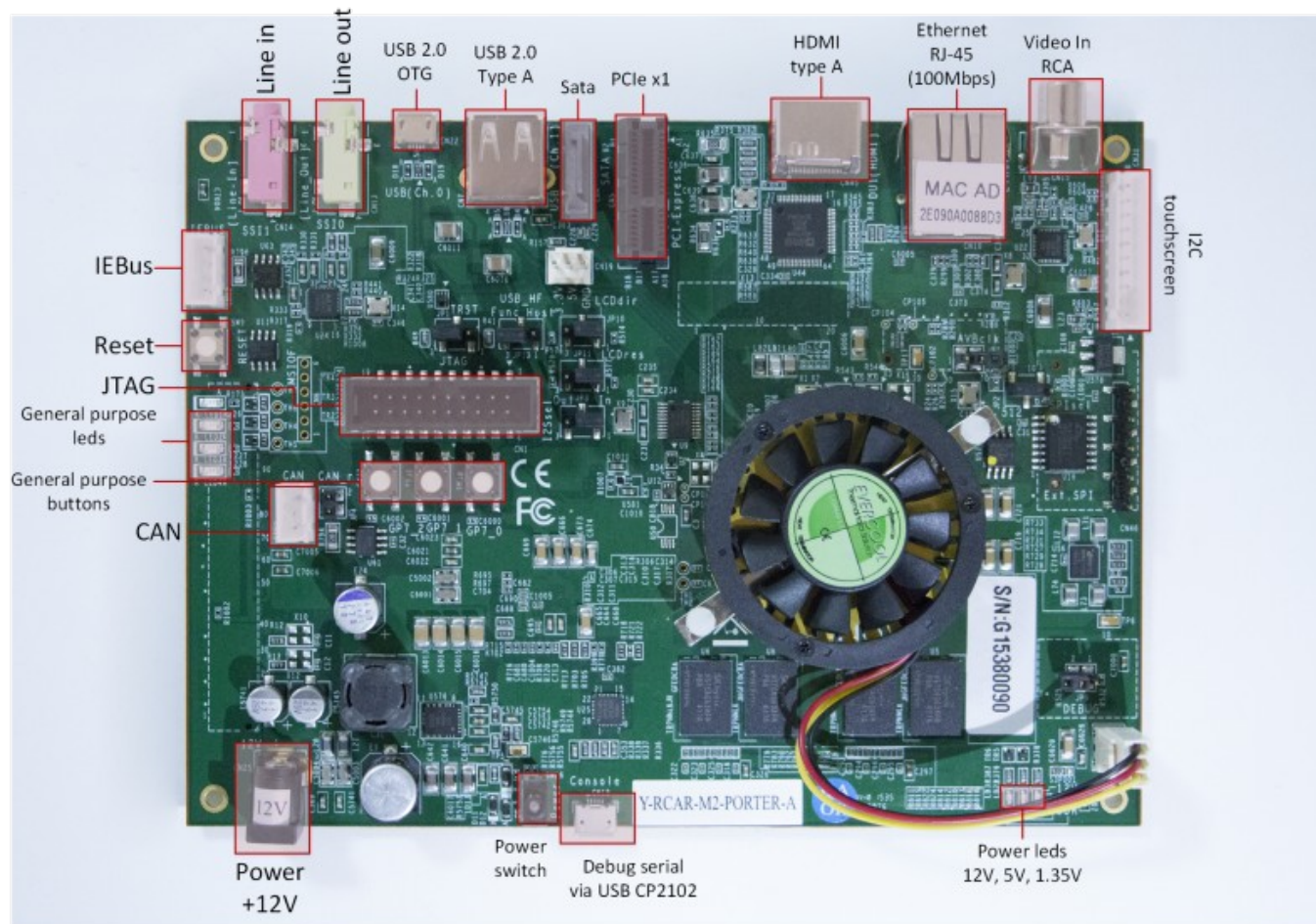


- *Homescreen*
- *AM/FM radio*
- *HVAC control*
- *Geolocation*
- *Media Player*
- *Phone*
- *Rear cameras*
- *Navigation helper*
- *Application manager*

# Introduction



## Sample : Renesas Porter (R-Car M2)



RENESAS

# Application development prerequisites



- For developers
  - support modern HTML5/JavaScript frameworks (*AngularJS, Foundation, Polymer...*)
  - any W3C-compliant application should work out-of-the-box !
  - consuming platform APIs should be straightforward & easy !
- For users
  - installing, uninstalling, starting, stopping... apps
  - application privileges rights will be clearly exposed
- Security concerns, for developers & users
  - privileges need to be enforced at system level

## Modern development methods

- Using modern JavaScript frameworks :
  - AngularJS <sup>[2]</sup>
  - Foundation <sup>[3]</sup>
  - Polymer <sup>[4]</sup>
- With a full-fledged IDE :
  - Eclipse
  - NetBeans
- with a dev/prod build system :
  - Gulp <sup>[5]</sup>
  - Grunt <sup>[6]</sup>
- and an adapted browser :
  - Chromium with LiveReload extension <sup>[7]</sup>





Foundation  
ZURB



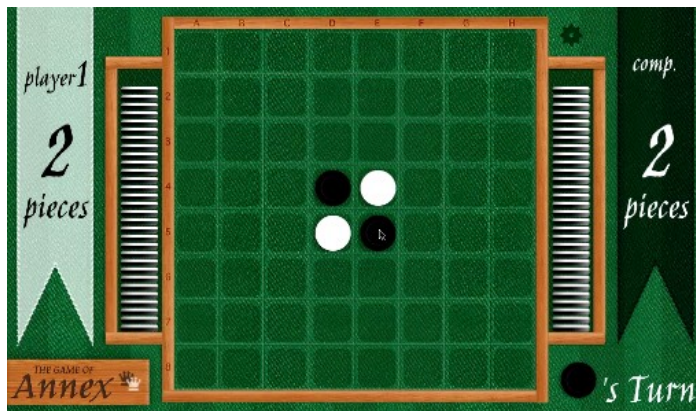


## Platform APIs as HTTP REST

Template : *http://<board>/api/<plugin>/<method>(?value=<var>)*

- *http://<board>/api/radio/mode?value=FM* : select FM mode 
- *http://<board>/api/radio/freq?value=110.2* : select 110.2 Hz 
- demo AM/FM Radio app is written using AngularJS ;
- platform glue is provided in plugins, written in C/C++, JavaScript ;
- developers should be able to write and provide their own plugins...
- ... but then, how do we :
  - package applications ?
  - enforce security ?

## Demos : HTML5/JS Radio, Annex, Rabbit



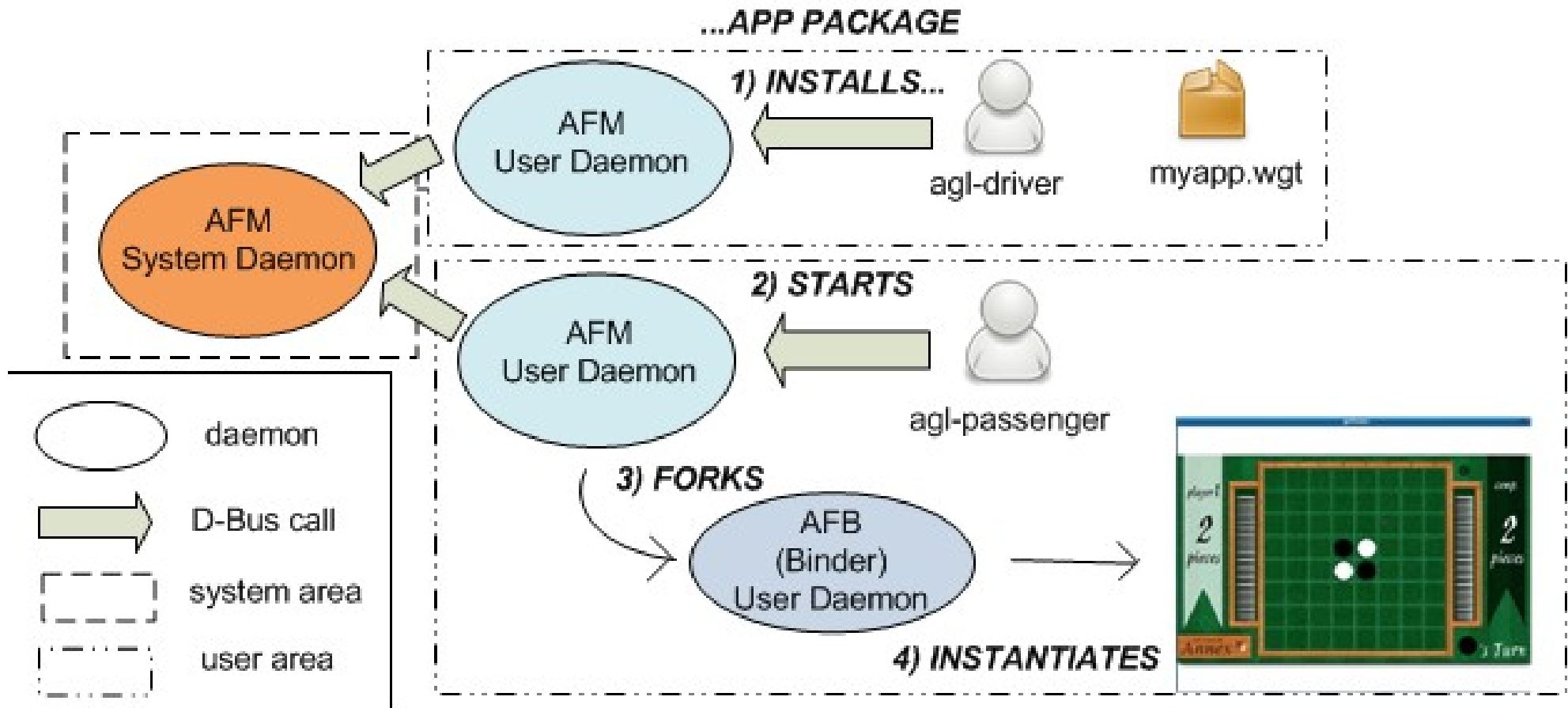




# Application Framework design

- Application Framework Manager <sup>[8]</sup>
  - System daemon : installs, uninstalls, list... applications system-wide
  - User daemon (1 per user) :
    - starts, stops, pauses... applications
    - when a HTML app starts, forks an **Application Framework Binder** with plugins & security context related to app category & privileges
- Application Framework Binder <sup>[9]</sup>
  - is a lightweight web server, based on libmicrohttpd <sup>[10]</sup>
  - loads platform plugins :
    - *Audio, AM/FM Radio, Media Server...*
  - provides platform APIs as HTTP REST APIs
- Web applications are displayed locally or remotely

# Application Framework platform design



## Application Framework design



## Demo : installing & running applications

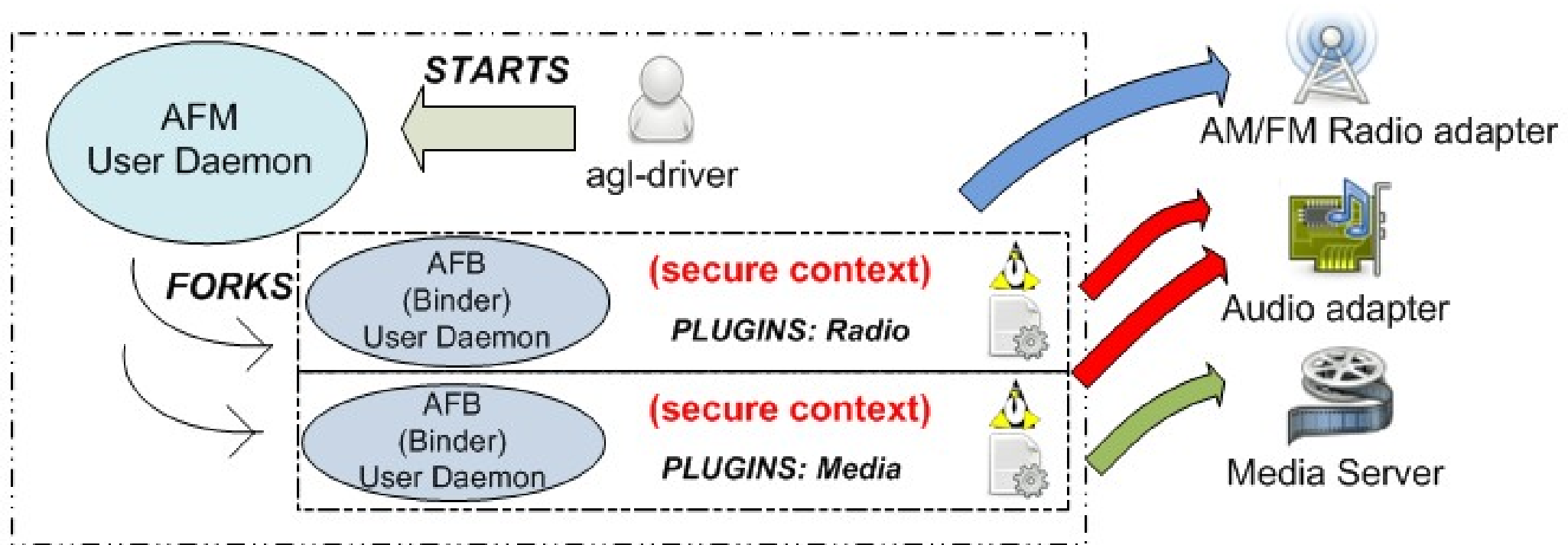
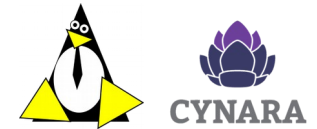


- *Uploading - Installing*
- *Starting*
- *Stopping*

## SMACK labels, Cynara policies

- SMACK (Simplified Mandatory Access Control Kernel) <sup>[11]</sup>
  - is a LSM (Linux Security Module)  
(others include : SELinux, AppArmor...)
  - associates security labels to files, processes and streams ;
  - “hard” security (system access denied on resource access)
- Cynara <sup>[12]</sup>
  - stores complex policies in databases ;
  - “soft” security (access is checked by framework) ;
- Security concerns, for developers & users
  - SMACK labels are attached to user-level Binder
  - Cynara is requested by Binder

# Privilege isolation through SMACK and Cynara



***Security for Application Framework Binder***



## Demo : exploitation attempt



# Annex

# Annex

# Links



- [1] HTTP REST : [https://en.wikipedia.org/wiki/Representational\\_state\\_transfer](https://en.wikipedia.org/wiki/Representational_state_transfer)
- [2] AngularJS : <https://angularjs.org/>
- [3] Foundation : <http://foundation.zurb.com>
- [4] Polymer : <https://www.polymer-project.org/>
- [5] Gulp : <http://gulpjs.com/>
- [6] Grunt : <http://gruntjs.com/>
- [7] LiveReload for Chromium :  
<https://chrome.google.com/webstore/detail/livereload/jnihajbhpnppcggbcgedagnkighmdlei>
- [8] Application Framework Manager : <https://github.com/iotbzh/afm-main>
- [9] Application Framework Binder : <https://github.com/iotbzh/afb-daemon>
- [10] libmicrohttpd : <https://www.gnu.org/software/libmicrohttpd/>
- [11] SMACK : <http://schaufler-ca.com/>
- [12] Cynara : <https://github.com/Samsung/cynara>

# Questions & Answers

## Q&A

# That's All Folks !

