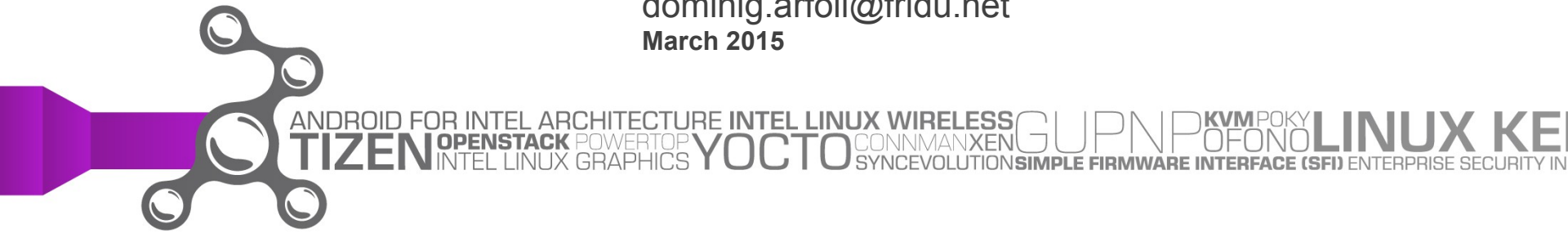
Ready made Recipes to add Security and Data Protection to a Yocto based Project reusing Tizen-Meta

Dominig ar Foll
(Intel Open Source Technology Centre)
dominig.arfoll@fridu.net
March 2015



Tizen-Meta

- IoT and Security
- What is Tizen
- Security Model for IoT
- How Security is enforced in Tizen
- What's next.

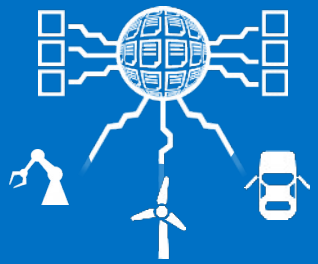
Dominig ar Foll
Intel Open Source Technology Centre

Intel's IoT Vision

INTELLIGENT DEVICES

Deliver Intelligence where needed to acquire

INTELLIGENT GATEWAYS



Unlocking and sharing valuable data in both legacy and

END TO END ANALYTICS

Solutions from device to cloud to deliver end-to-end

IoT Solutions are End-to-End Distributed Applications

IoT Has Security and Privacy Concerns

Venture Beat News: “The Internet of Things will be vulnerable for years, and no one is incentivized to fix it”

CMS Wire: “Top 5 IoT security concerns: Privacy, Authentication, Transport Encryption, Web Interface, Insecure Software”

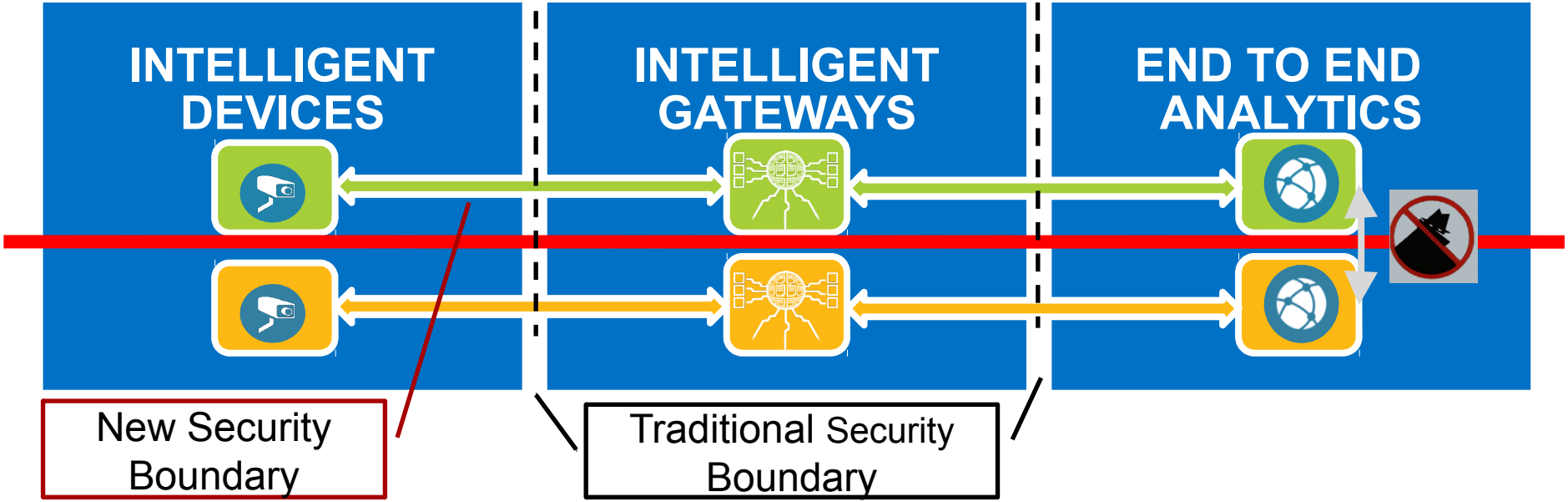
Wired: “The Internet of Things has Arrived – And so have Massive Security Issues”

The Inquirer: “The Internet of Things needs a security model to protect user data”

CSO: “Mainstream Internet of Things raising consumer security, privacy concerns”

Dominig ar Foll
Intel Open Source Technology Centre

Distributed IoT Applications = Distributed Threats

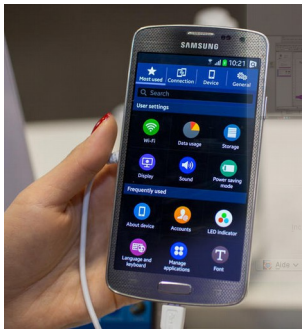


Dominig ar Foll
Intel Open Source Technology Centre

Tizen, an OS for Connected Devices

Multiple profiles:

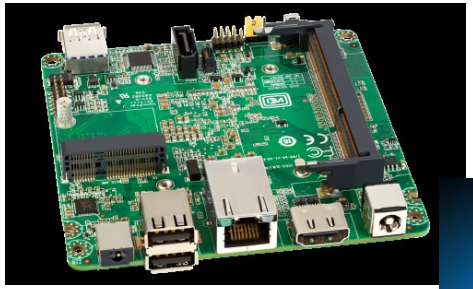
- Mobile
- IVI
- TV
- Household equipments
- Wearables



Dominig ar Foll
Intel Open Source Technology Centre

Hacker Friendly supported platforms

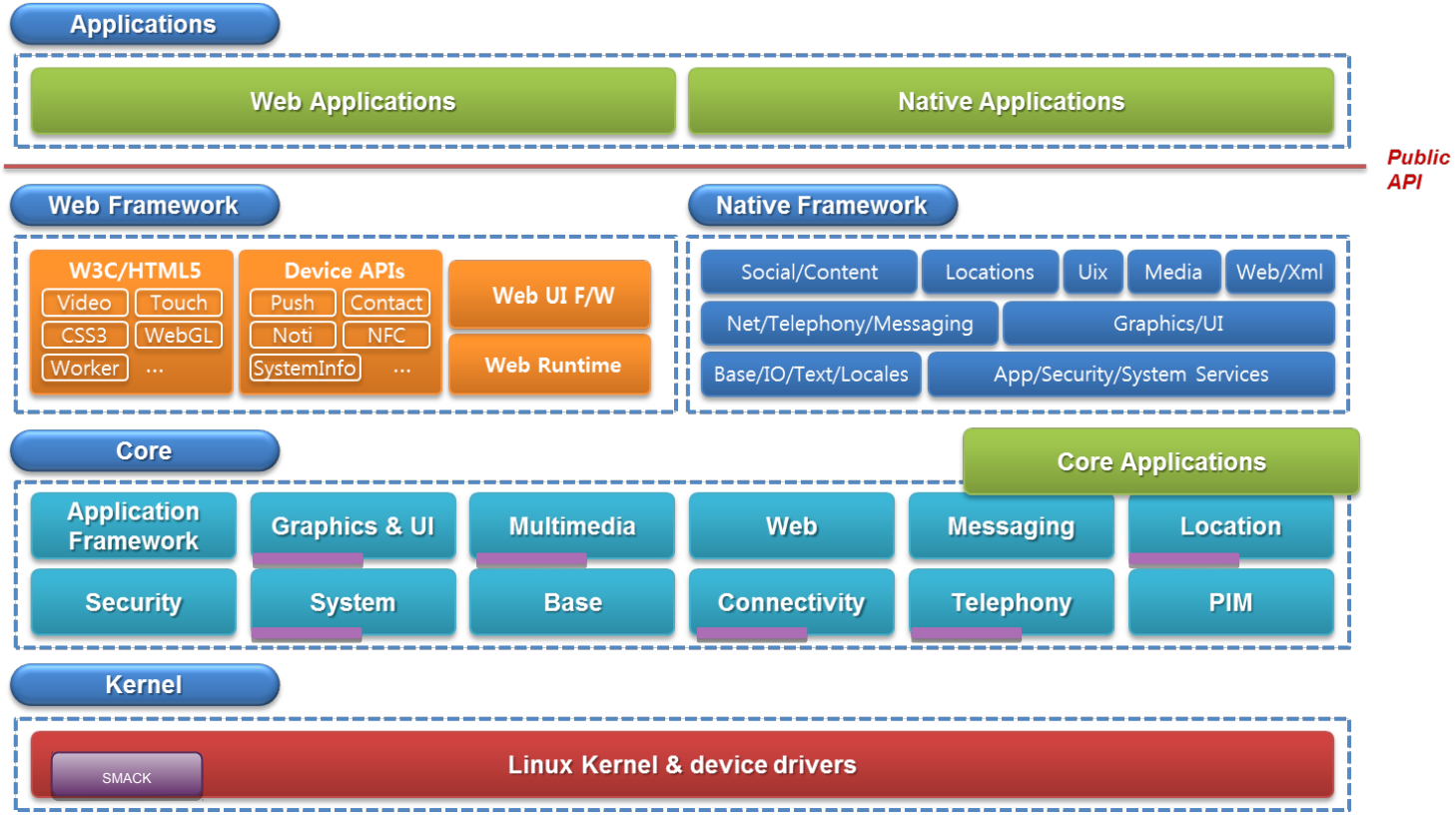
- Intel
  - NUC
  - MinnowBoard Max
  - Galileo-2



- ARM
  - Odroid U3

Dominig ar Foll
Intel Open Source Technology Centre

Architecture Overview (Mobile Profile)



Dominig ar Foll
Intel Open Source Technology Centre

Tizen Connectivity*

- Bluetooth 4 (Low energy)
- Ethernet AV
- Wifi P2P
- GSM 3G/4G
  - Phone
  - Messages
  - Data
- IoTivity
- Tethering
- Hand Free support
- Miracast
- DLNA
- Shared Drive
- Multi Screen

* hardware dependent

Dominig ar Foll
Intel Open Source Technology Centre

4 kinds of security

- **Isolation of the users and applications**
  - An application cannot access the data of other application
  - How? Use of Smack and DAC
- **Restriction of the services**
  - An application cannot access the services without authorisation
  - How? Use of Smack and Cynara
- **Restriction of the network**
  - An application cannot access network without authorisation
  - How? Use of Smack and netfilter
- **Integrity**
  - Code and stable Data integrity enforcement
  - How ? check by Kernel

Dominig ar Foll
Intel Open Source Technology Centre

Security Model

- Reduce all surfaces of Attack
- Enforce a minimum privilege policy
- Reduce on and off line Attack
- Provide a ready and easy to use solution
- Protect Code, Data and Connections
- Deliver with existing tools

Dominig ar Foll
Intel Open Source Technology Centre

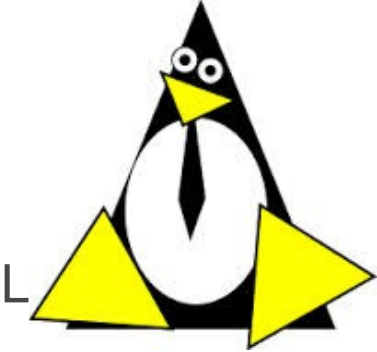
Isolation of applications

- The file system is cut in user parts using traditionnal Unix DAC uid partition
  - A user can access its own $HOME
  - A user cannot access the home of other users
- The file system is cut in application parts using the Smack MAC labels
  - Each application has its own label
  - An application can only access its own labelled files

	AppX alice	AppY alice	AppX bob	AppY bob
AppX alice	**YES**	NO (MAC)	NO (DAC)	NO (DAC+ MAC)
AppY alice	NO (MAC)	**YES**	NO (DAC+ MAC)	NO (DAC)
AppX bob	NO (DAC)	NO (DAC+ MAC)	**YES**	NO (MAC)
AppY bob	NO (DAC+ MAC)	NO (DAC)	NO (MAC)	**YES**

Dominig ar Foll
Intel Open Source Technology Centre

Short overview



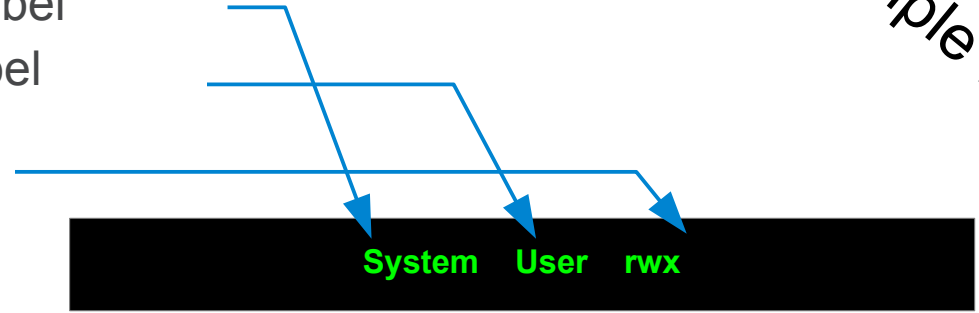
- The author of Smack is mainly Casey Schaufler.
- In Linux since kernel 2 6 25 – 17 April 2008 – as a LSM (Linux Security Module)
- Evolving since this first days.
- Inside Tizen since the first days (2012).
- Use extended file attributes to store data relating to files.
- Controlled via a filesystem interface: smackfs.
- Controls accesses of processes to files, IPC, sockets and processes (ptrace, signals, ...).
- Controls CIPSO labelled IPV4 packets

Dominig ar Foll
Intel Open Source Technology Centre

The Smack rules

- Smack's rules have 3 items:
  - the subject's label
  - the object's label
  - the access

Simple !!!



This rule tells to allow **read**, **write** and **execute** access to objects labelled **User** for the processes labelled **System**.

What are labels? **What are subjects?** **What are objects?** **How to set?**

Dominig ar Foll
Intel Open Source Technology Centre

Integrity

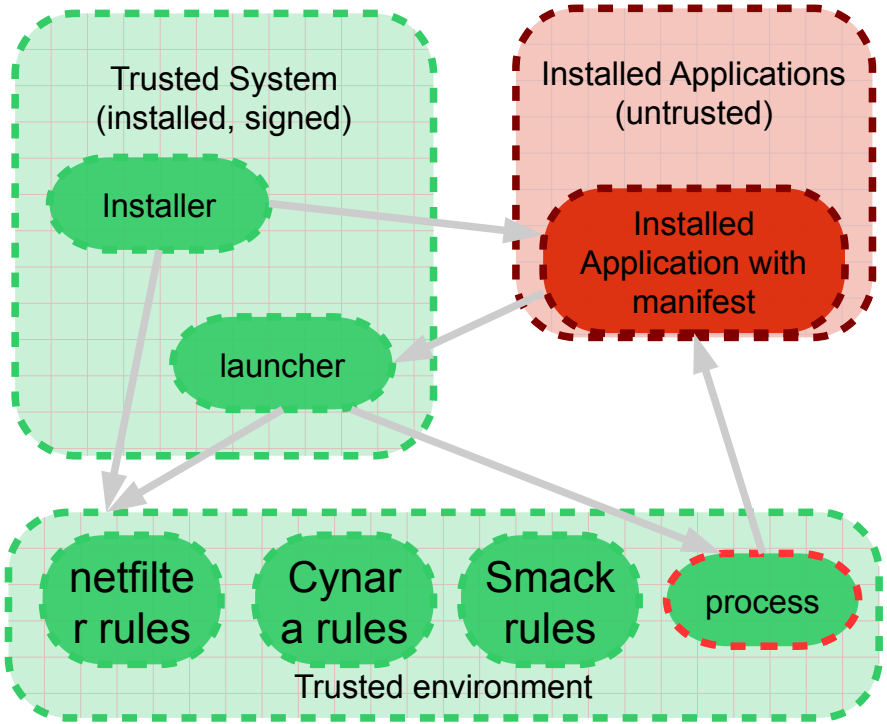
- Policy based on:
  - Path
  - File owner
  - Process owner
  - File permissions (executable/non-executable)
  - LSM labels
  - Action (open/exec)

- Possible runtime policy management (C API):
  - Get current policy
  - Set policy from file
  - Set policy from list of rules (**char)
- Documentation
  - https://wiki.tizen.org/w/index.php?title=Security:IntegrityMeasurement

Dominig ar Foll
Intel Open Source Technology Centre

Application live cycle

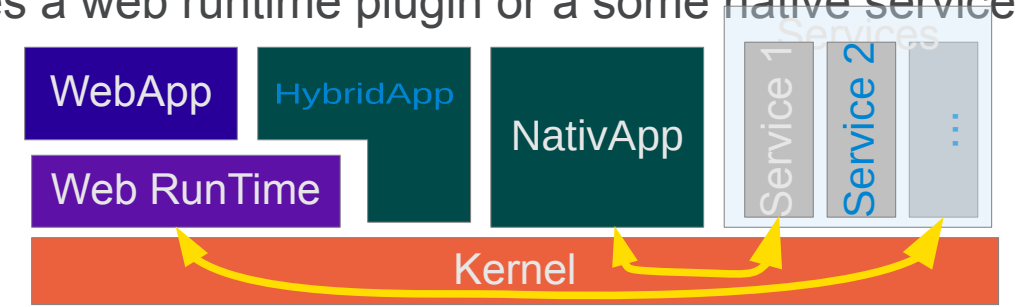
- Applications are installed by an installer
  - The installer enable the application, configure the system according to the manifest.
- Applications are launched by a launcher
  - The launcher prepare the environment in agreement with the manifest and launch the application in the trusted environment.



Dominig ar Foll
Intel Open Source Technology Centre

3 kinds of applications

- The web applications
  - Written in HTML5/CSS3/JAVASCRIPT
- The native applications
  - Written in any language including C/C++
- The hybrid applications
  - Mainly written in HTML5/CSS3/JAVASCRIPT
  - Includes a web runtime plugin or a some native service or application



Dominig ar Foll
Intel Open Source Technology Centre

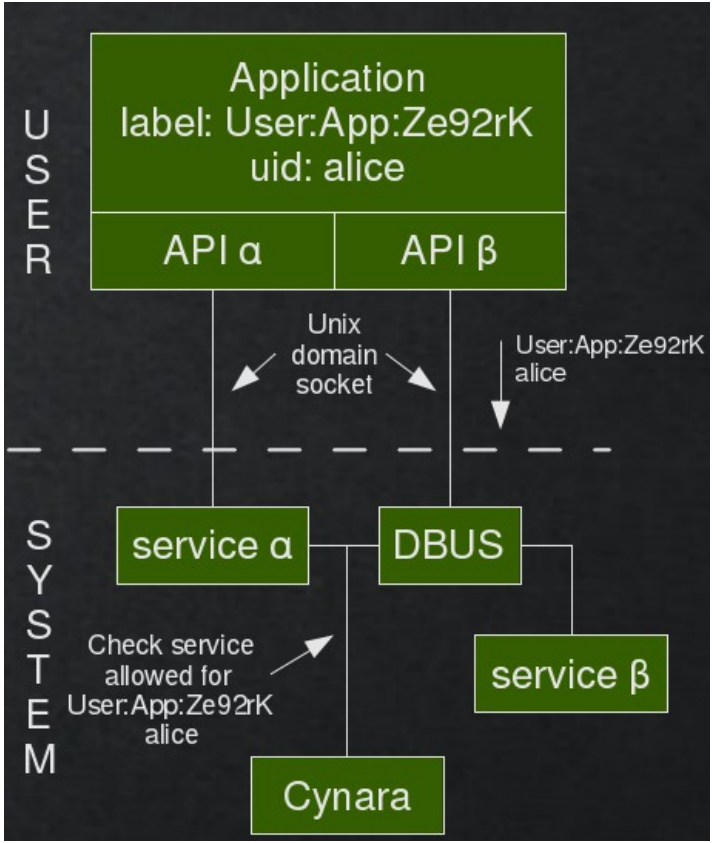
Restriction of access to services

- Apps must provide a manifest declaring required services
- Access to Service is control by the OS from Manifest
- Control enforced for :
  - Enabled Daemon
  - D-Bus
  - Devices
  - Files
- Under investigation
  - Access to the network using MAC and netfilter and name spaces
  - Shared Libraries
  - Name spaces

Dominig ar Foll
Intel Open Source Technology Centre

Restriction of services

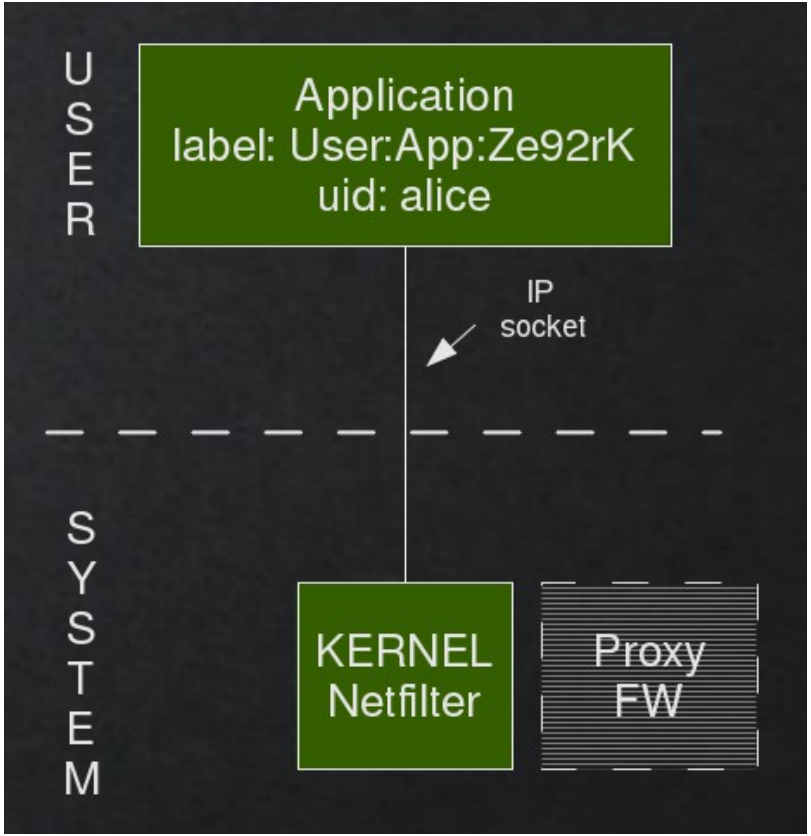
- The invocations of services are using UDS
- The UDS expose the credentials of the pair: Smack label, uid, pid
- Before servicing, the service ask cynara for the authorisation using the smack label, the uid and some session id
- Cynara scans its database and reply
  - A fast cache is enable
  - Cynara can request user decision through HMI



Dominig ar Foll
Intel Open Source Technology Centre

Restriction of network

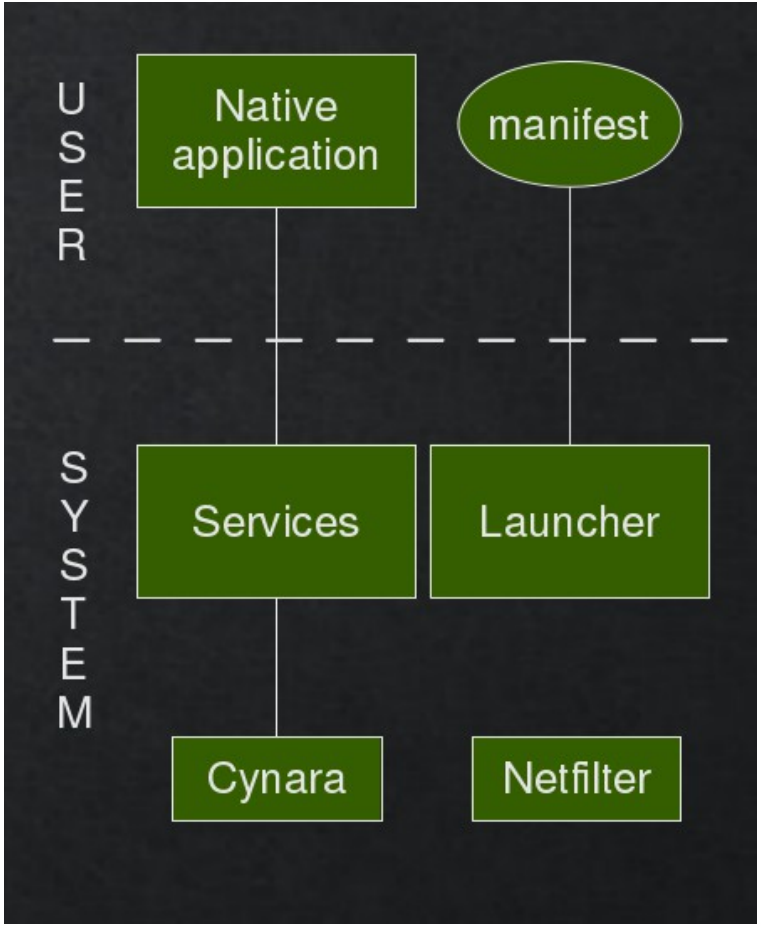
- To be finalised
- Access to the network are filtered using DAC and netfilter
- A filtering proxy-firewal may be also implemented for parental control.



Dominig ar Foll
Intel Open Source Technology Centre

The native applications

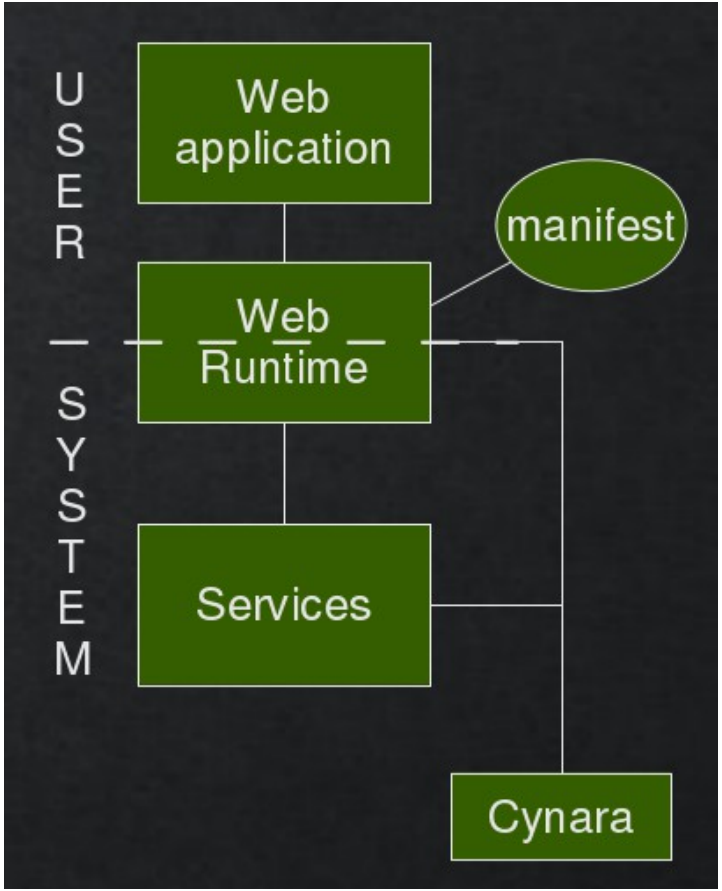
- The applications cannot be launched directly
- The launcher is in charge of setting the runtime environment of applications
  - Specific gid
  - Netfilter data
- Services
  - D-Bus filtering
  - Service daemon



Dominig ar Foll
Intel Open Source Technology Centre

The web applications

- As natives plus:
- The Web runtime (crosswalk) is in charge of enforcing the security of the application
- Because of its model, the Web Runtime includes a trusted part (in the system space)
- The Web runtime ensure respect of the Content Security Policy (W3C)



Dominig ar Foll
Intel Open Source Technology Centre

Restriction of shared files

- Some files (like /dev/camera) are shared to users but restricted by privileges. Note that this resources can be subject to resource management (murphy)

- When no service is used as a mediator to access this resources, then:
  - No Cynara check can be performed.
  - For this specific shared files, the access is restricted by DAC and gid to a specific group.
  - The launcher is in charge to add the group to the launched application that requires following the cynara diagnostic

Dominig ar Foll
Intel Open Source Technology Centre

How to share files?

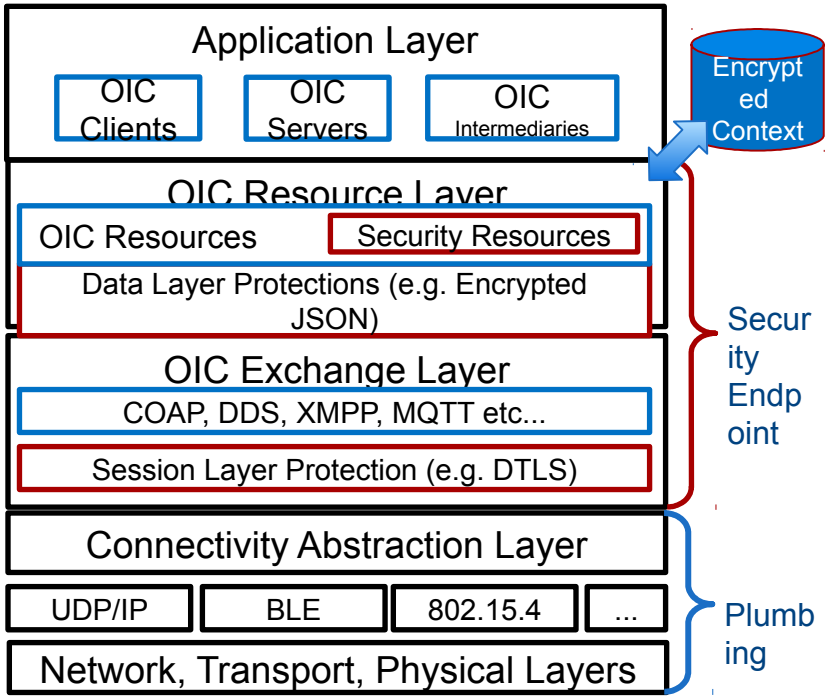
- When files must be shared acros applications (example: an image, a pdf, a text, …) the file is copied to a directory dedicated to sharing:
  - One sharing directory per user
  - One global sharing directory
- When files must be transmitted from one user to an other, a directory specific to the destination user is used.

Dominig ar Foll
Intel Open Source Technology Centre

IoT Frameworks enforce end-2-end security

(IoTivity, Allseen, Thread etc...)

Network, transport and even session layer security are less relevant



Security Resources

- Access control policies and access enforcement
- Credentials, roles, groups, pairing and identity
- 'Device' ownership
- Secure configuration of resources

OS Dependencies

- Stack instance isolation
- Resource layer ←→ app layer isolation
- Encryption key storage
- Stack instance integrity / secure boot

How applications collaborate?

- Applications sharing the same origin (as signed by a certificate) can :
  - Share some common files
  - Communicate using Message Port service

Dominig ar Foll
Intel Open Source Technology Centre

Probable Future Moves

- / as Readonly with OverlayFS (from Kernel 3.18)
- “un-root” all services
- Containers for each Apps
- Containers for critical Middleware
- Dynamic Integrity check including Kernel (using HW)

Dominig ar Foll
Intel Open Source Technology Centre

Try Tizen Meta

- HowTo
  https://wiki.tizen.org/wiki/Tizen_on_yocto
- Support
  https://lists.tizen.org/listinfo/dev
- Code
  https://review.tizen.org/gerrit/#/admin/projects/scm/bb/meta-tizen
- Bugs
  https://bugs.tizen.org/jira/browse/BTY

Dominig ar Foll
Intel Open Source Technology Centre


Q & A

Gulf of Morbihan, south of Brittany, France

The Smack vocabulary

- **Labels** are just text (of valid ASCII characters) without any special meaning: they are compared to equality (case sensitive: a≠A).
- **Subjects** are running processes: any running process has a smack label.
- **Objects** are **files**, **IPC**, **sockets**, **processes**.
- The label of a running process is called its **context**.
  - The commands id, ps (option -Z or -M), ls (option -Z) are prompting the contexts of the current process, the running processes, the files.
- The grantables **access modes** are: **read** (r), **write** (w), **execute** (x), **append** (a), **lock** (l), **transmute** (t).

Dominig ar Foll
Intel Open Source Technology Centre

Setting Smack

- How to set context? You can't! Except if you have the capability CAP_MAC_ADMIN.
-
```
# chsmack --access label file
# echo -n label > /proc/$$/attr/current
```
- How to set rules? You can only reduce accesses for the current thread (inherited by cloning). But if you have the capability CAP_MAC_ADMIN, you can change all rules.

```
# echo “subject object rwt” > /sys/fs/smackfs/load-self2
# echo “subject object rwt” > /sys/fs/smackfs/load2
# echo “subject object rwt” > smackload
```


Dominig ar Foll
Intel Open Source Technology Centre