Aleksander Zdyb

Modern Security Model for Linux Operating Systems

Aleksander Zdyb

SOFTWARE ENGINEER
TIZEN PLATFORM SECURITY

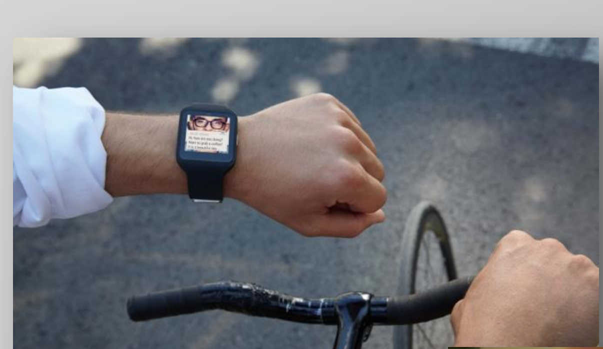
a.zdyb@samsung.com https://github.com/azdyb

Agenda

- Briefly about security requirements
- About Tizen operating system
- Dedicated security model
- Application lifecycle
- Summary

About security requirements

Common, smart devices

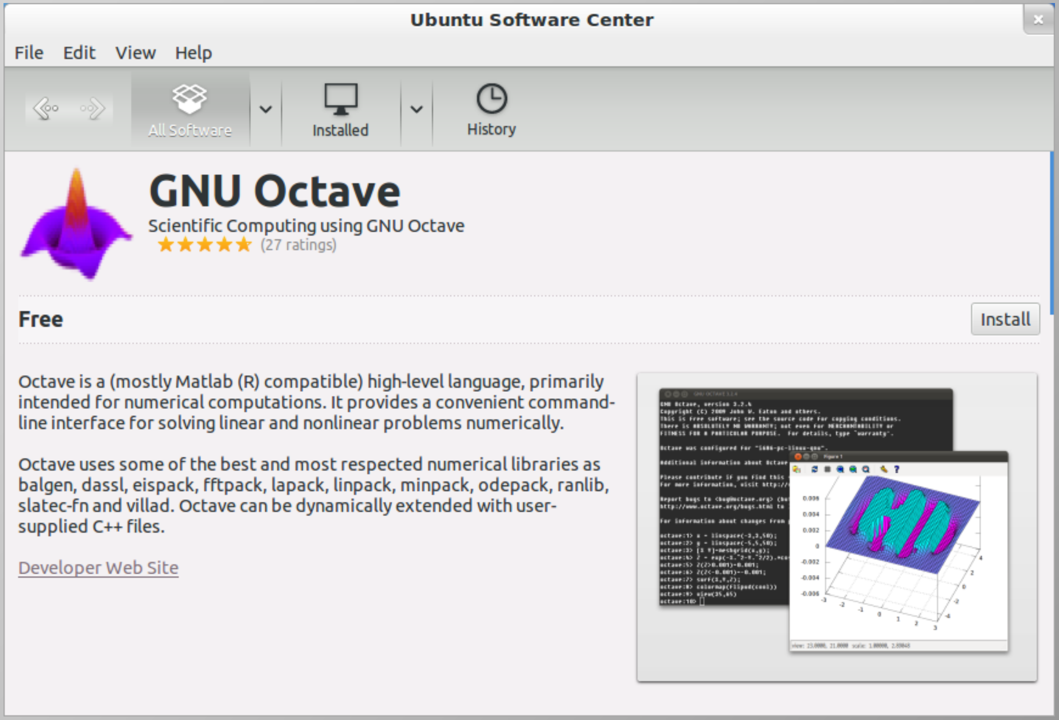


(CC) Stiftelsen Elektronikkbransjen

(CC) Intel Free Press

(CC) Sascha Müsse

This is what we all know



GNU Octave

Scientific Computing using GNU Octave

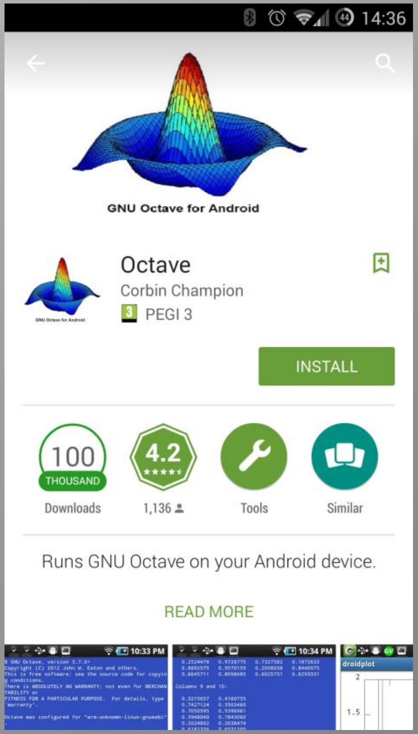
★★★★★ (27 ratings)

Free

Octave is a (mostly Matlab (R) compatible) high-level language, primarily intended for numerical computations. It provides a convenient command-line interface for solving linear and nonlinear problems numerically.

Octave uses some of the best and most respected numerical libraries as balgen, dassl, eispack, fftpack, lapack, linpack, minpack, odepack, ranlib, slatec-fn and villad. Octave can be dynamically extended with user-supplied C++ files.

Developer Web Site



Octave

Corbin Champion

PEGI 3

100 THOUSAND Downloads

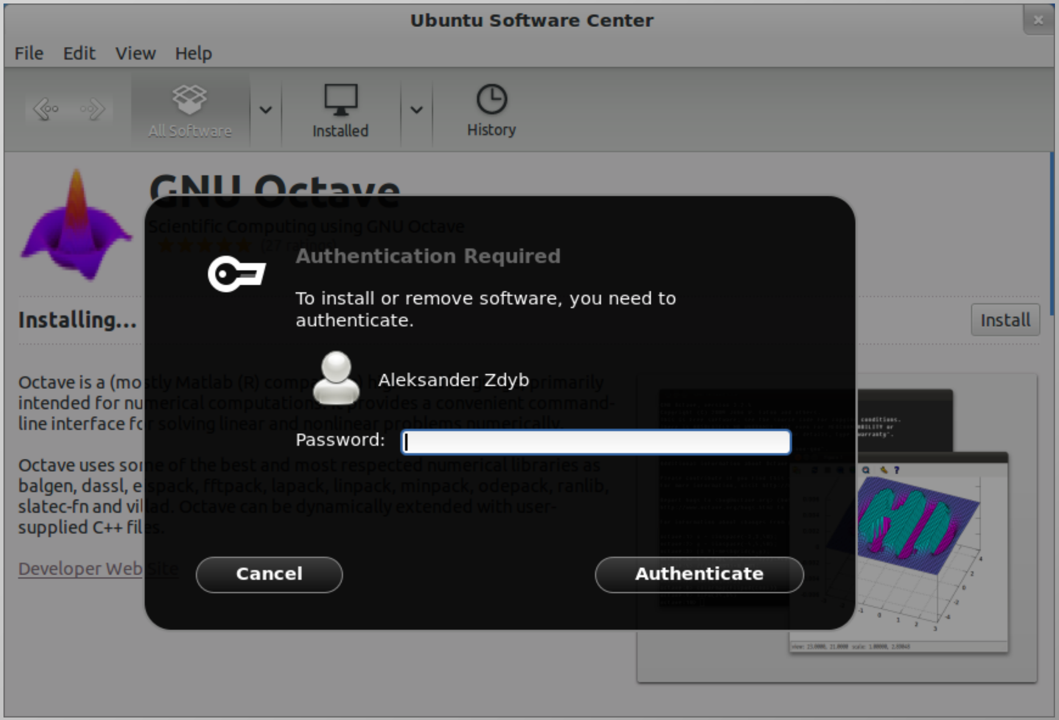
4.2 ★★★★★ 1,136

Tools

Similar

Runs GNU Octave on your Android device.

This is what we all know



Authentication Required

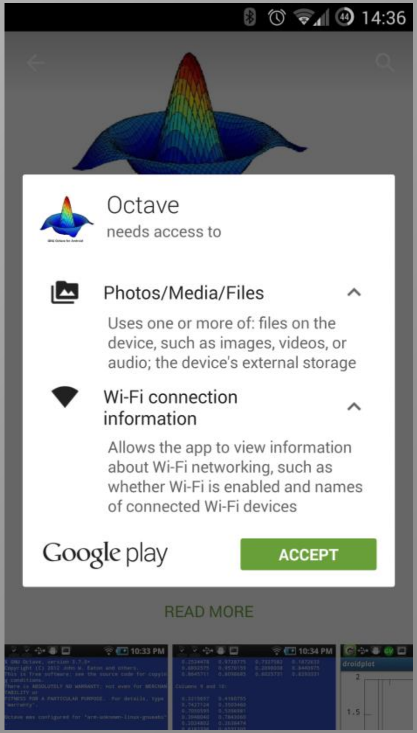
To install or remove software, you need to authenticate.

Aleksander Zdyb

Password:

Octave is a (mostly Matlab (R) compatible) high-level language, primarily intended for numerical computations. It provides a convenient command-line interface for solving linear and nonlinear problems numerically.

Octave uses some of the best and most respected numerical libraries as balgen, dassl, eispack, fftpack, lapack, linpack, minpack, odepack, ranlib, slatec-fn and villad. Octave can be dynamically extended with user-supplied C++ files.



Octave
needs access to

Photos/Media/Files
Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage

Wi-Fi connection information
Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices

Security in embedded systems

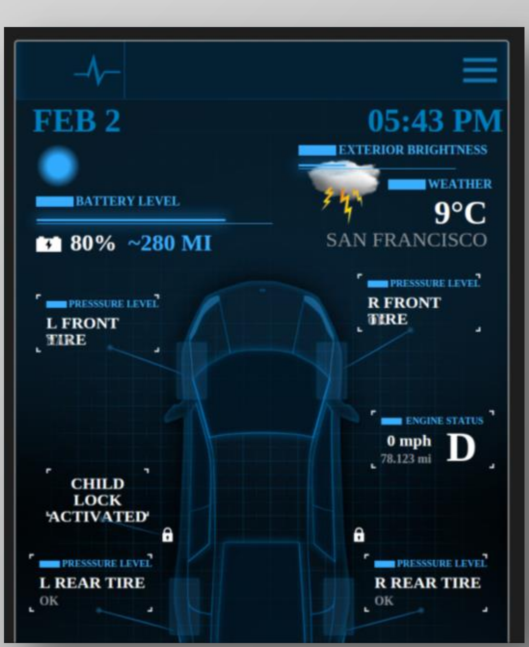
- Classic approach: software acts on behalf of user to full extent
- Usage of many kinds of privileges is more and more common
- There is a conflict between privileges granularity
  and comfort of usage and administration

About Tizen

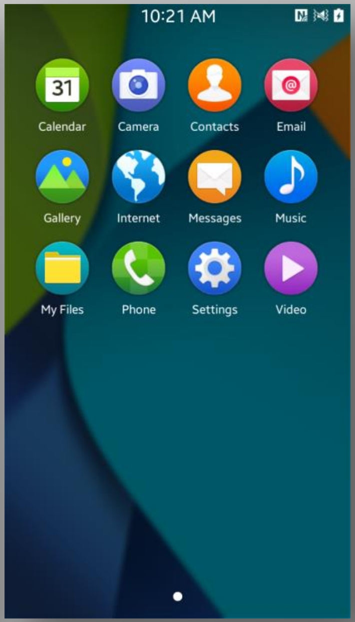
About Tizen

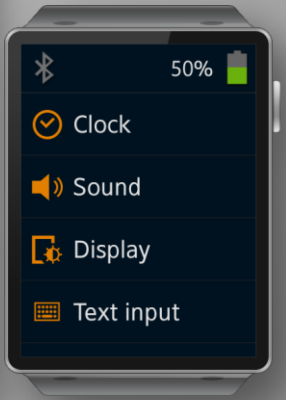
- Modern operating system for embedded devices
- A Linux distribution
- Developed by Open Source community
- Main contribution from Samsung at the moment

Where to meet Tizen?



wiki.tizen.org





- Smartphones, smartwatches, smart TVs
- IVI systems (In-Vehicle Infotainment)
- And more

TIZEN 2.x and TIZEN 3.0

TIZEN 2.x

- Commercially released in many Samsung's devices (smartwatches, smart TVs, smartphones)
- Security ensured with classic mechanisms of Linux

TIZEN 3.0

- Still in developent
- Works on ODROID XU3 (arm), MinnowBoard MAX (x86_64) and other architectures
- Modern, dedicated security model

Services, resources and privileges

Operating system governs services and resources

Example services and resources

- E-mail
- Camera
- Networking

Operating system governs services and resources

Example services and resources

- **E-mail**
- **Camera**
- **Networking**

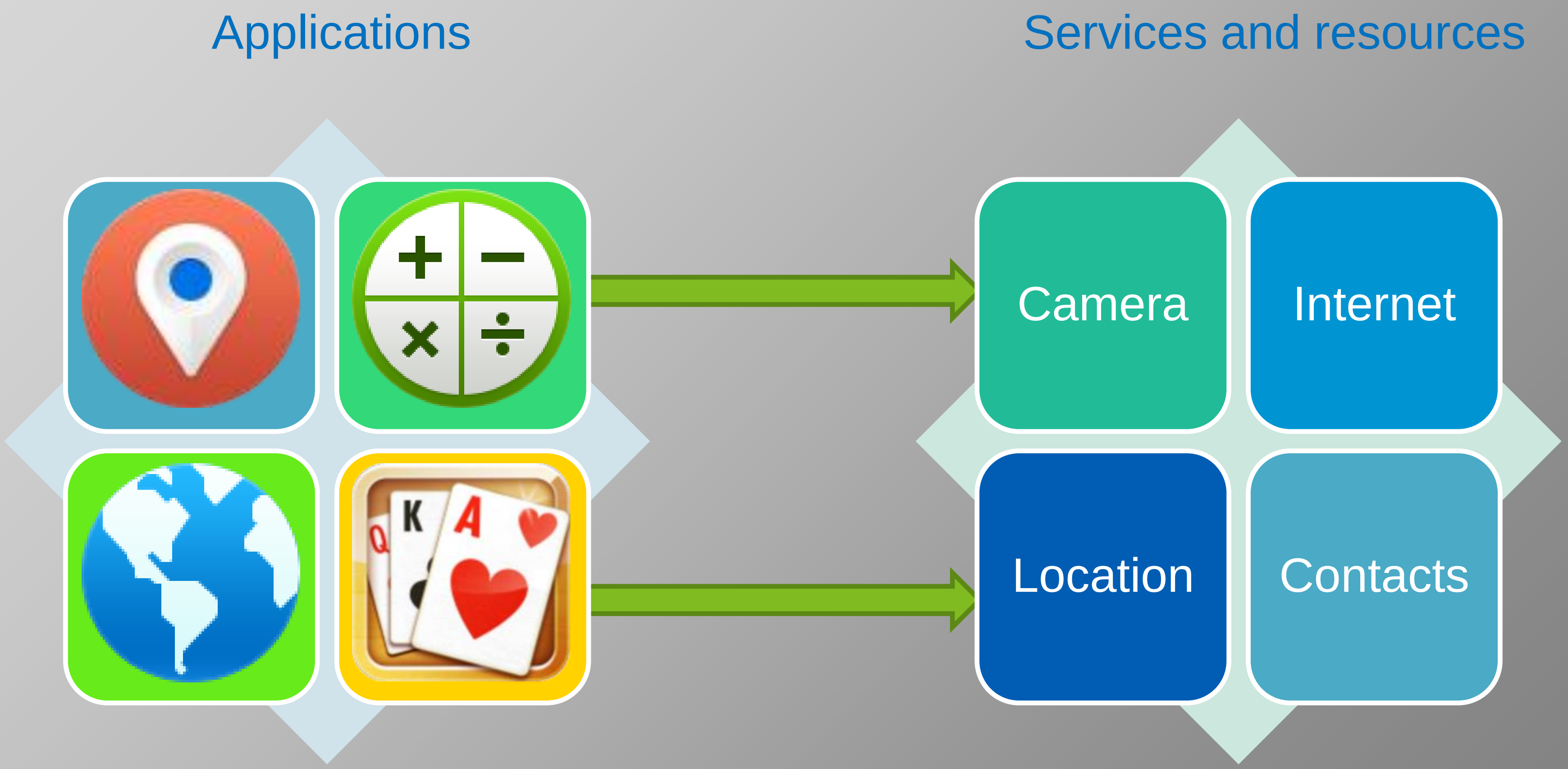
Related privileges

- Reading, sending messages
- Contacts preview

- Taking photos
- Browsing pictures

- Accessing remote hosts
- Usage of different protocols

Operating system governs services and resources



Applications

Services and resources

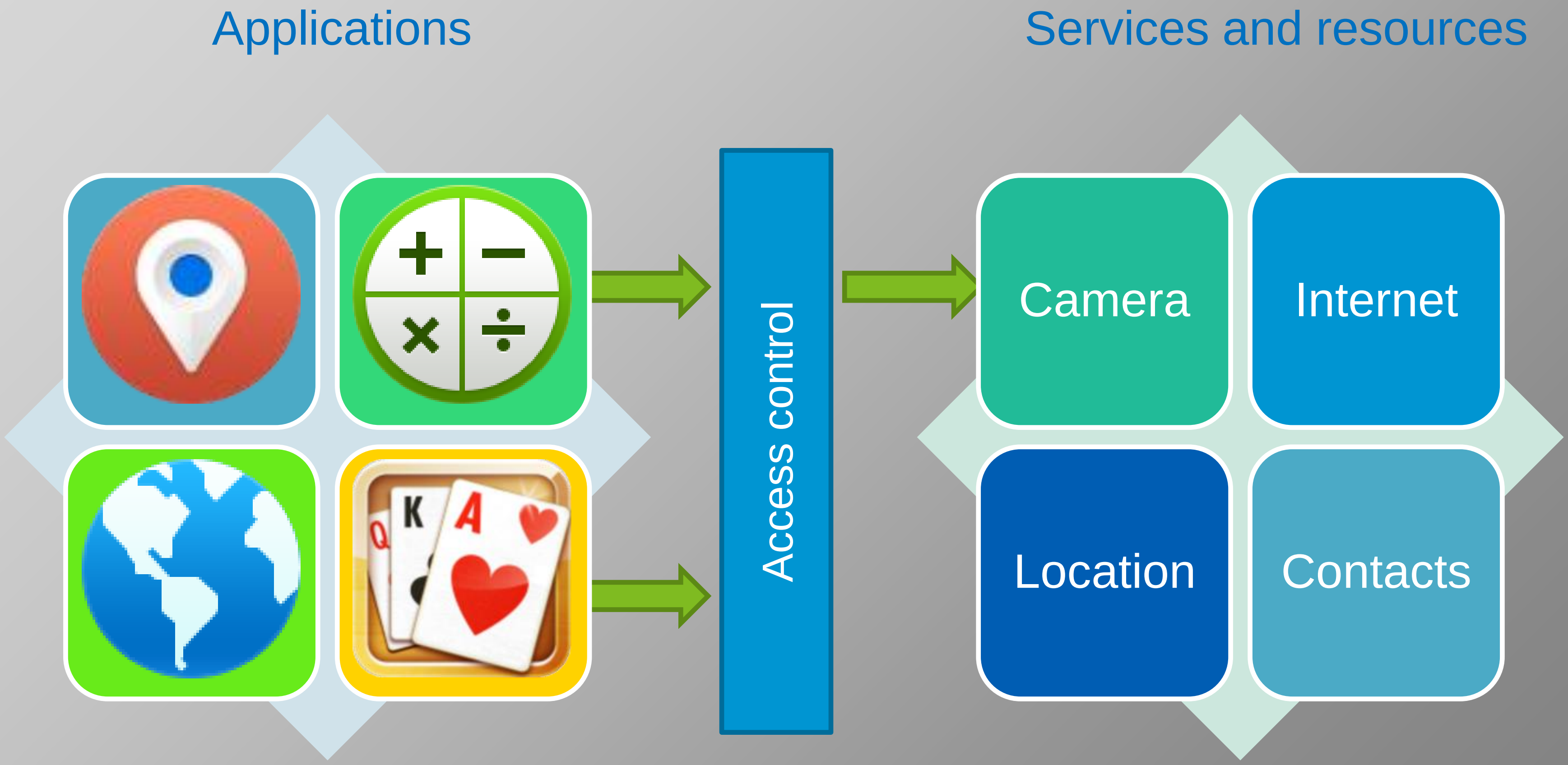
Camera

Internet

Location

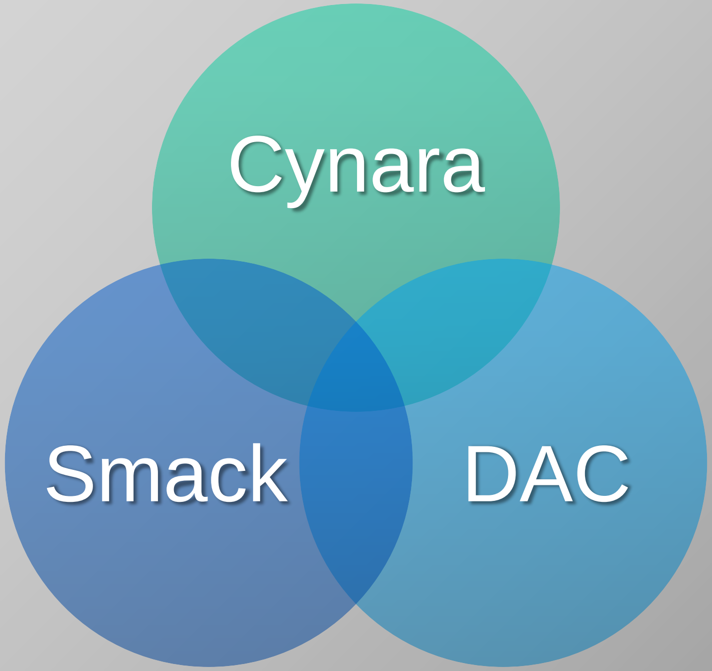
Contacts

Operating system governs services and resources



Dedicated Security Model

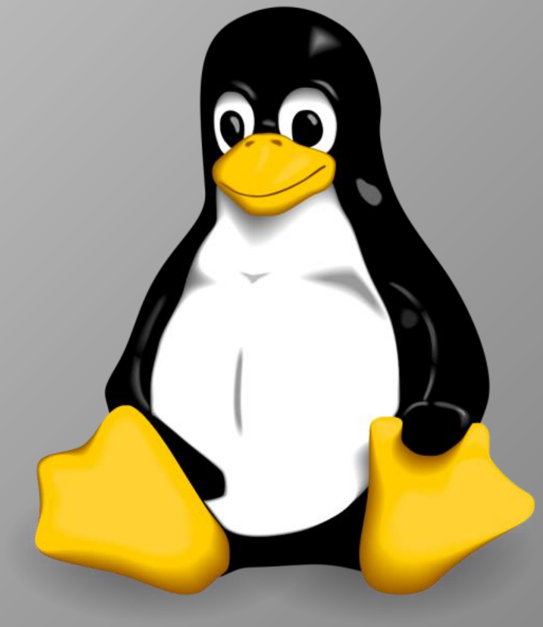
Three pillars of security



- DAC – Discretionary Access Control (classic access control system)
- Smack – Simplified Mandatory Access Control Kernel (one of LSMs)
- Cynara – dedicated privilege checker (userspace)

1st pillar of security: DAC – separation of users

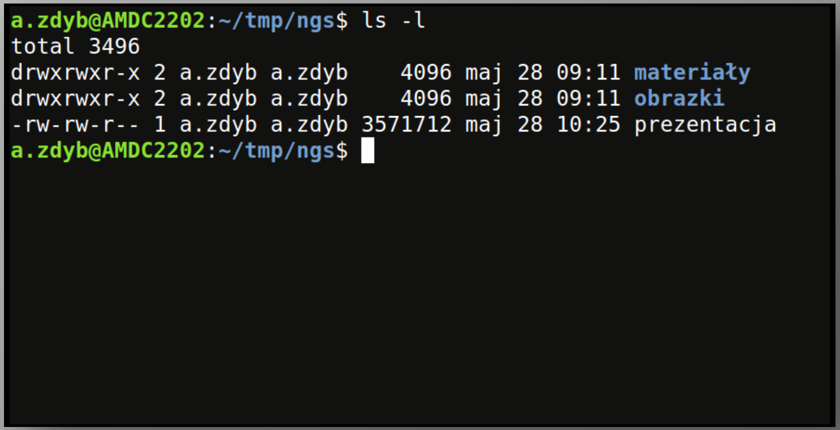
- Protects resources on filesystem
- Access control set by owner of the resource
- Access types: r w x
- Subject is identified by its id and groups it belongs to



Larry Ewing and The GIMP

1st pillar of security: DAC – separation of users

- Protects resources on filesystem
- Access control set by owner of the resource
- Access types: r w x
- Subject is identified by its id and groups it belongs to



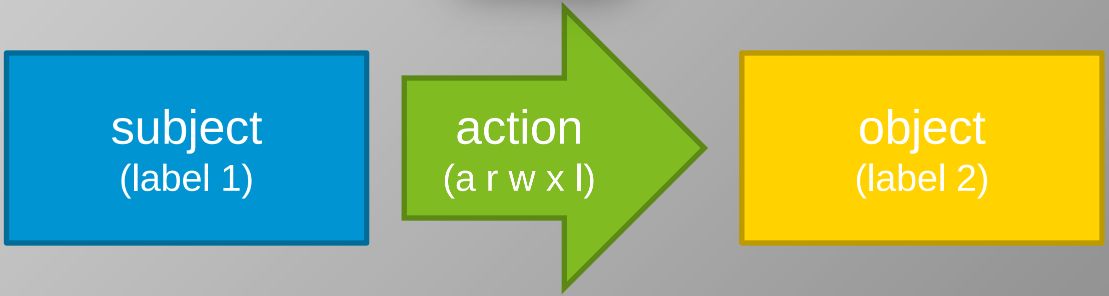
```
a.zdyb@AMDC2202:~/tmp/ngs$ ls -l
total 3496
drwxrwxr-x 2 a.zdyb a.zdyb    4096 maj 28 09:11 materiały
drwxrwxr-x 2 a.zdyb a.zdyb    4096 maj 28 09:11 obrazki
-rw-rw-r-- 1 a.zdyb a.zdyb 3571712 maj 28 10:25 prezentacja
a.zdyb@AMDC2202:~/tmp/ngs$
```

2nd pillar of security: Smack – separation of processes

- Both object and subject are identified by their labels
- Access control is set by administrator
- Access types: a r w x t l

(GFDL) Casey Schaufler

2nd pillar of security: Smack – separation of processes



subject
(label 1)

action
(a r w x l)

object
(label 2)

2nd pillar of security: Smack – separation of processes

Floor (_)

- Read-only system directories
- Kernel’s helper processes

System

- /run, /dev, /var/log
- System services

User

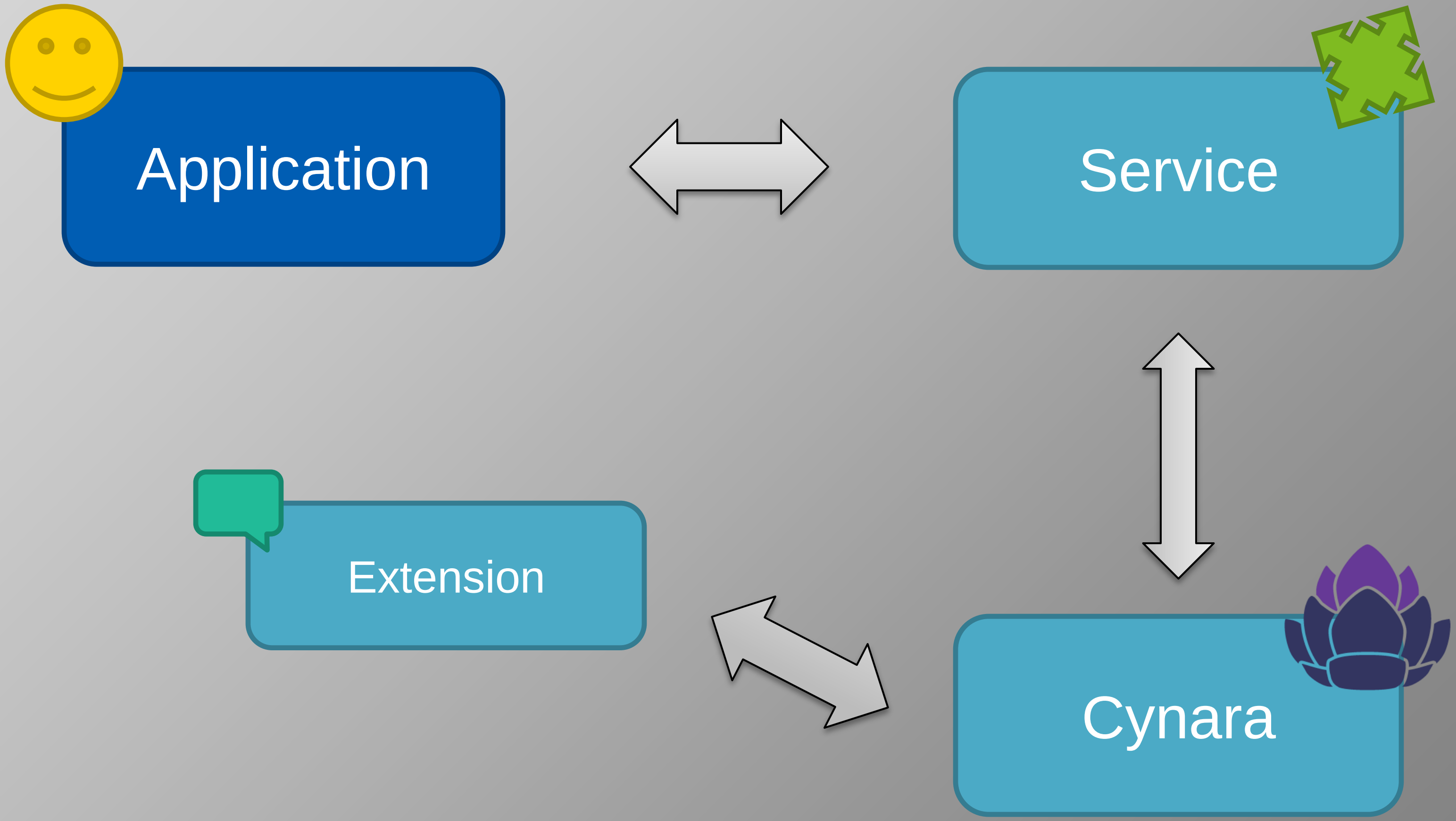
- Home directories
- Launcher
  and users’ services

Domains are sets of labels with common prefix.
There are other labels, like System::Shared, User::Home and more.

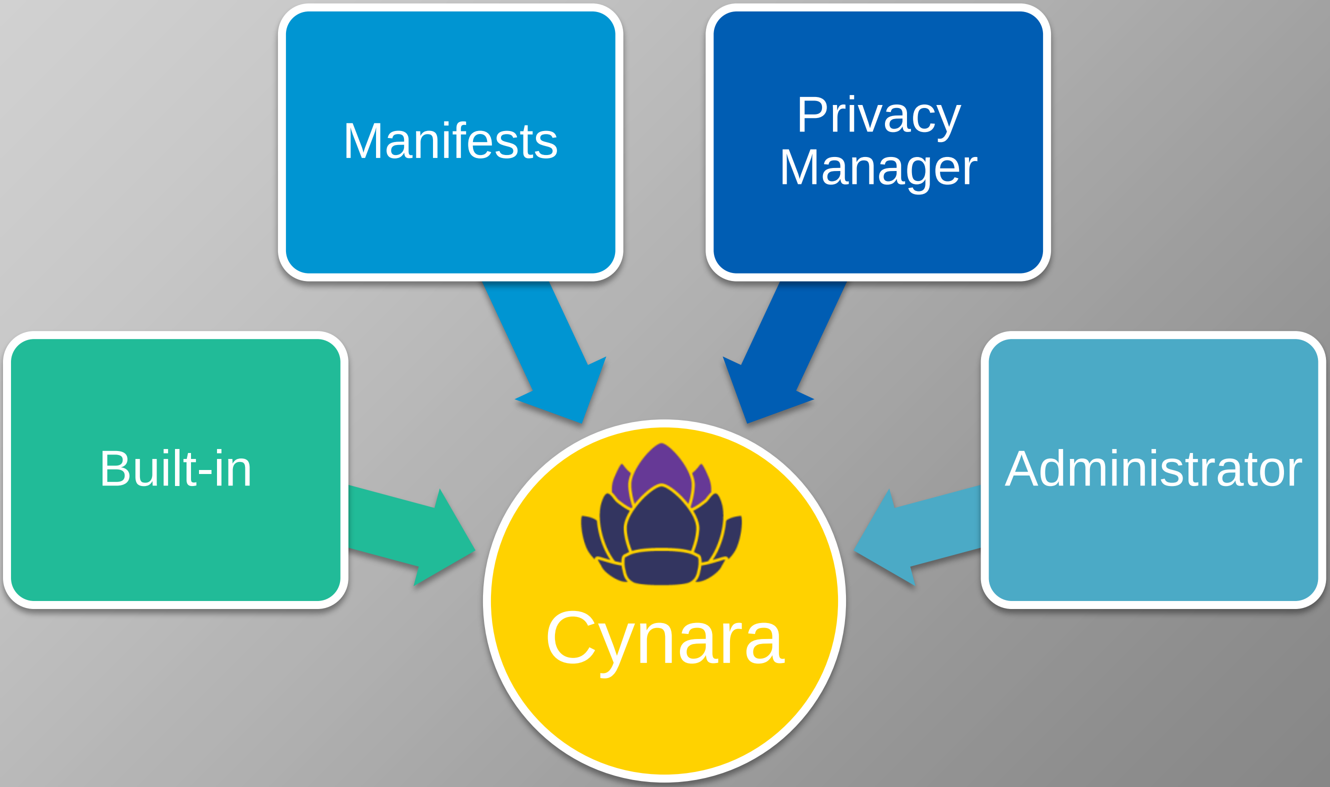
3rd pillar of security: Cynara

- System service keeping and managing security policies
- Dedicated solution for Tizen 3.0
- Generic – can be easily deployed in other Linux distributions

3rd pillar of security: Cynara

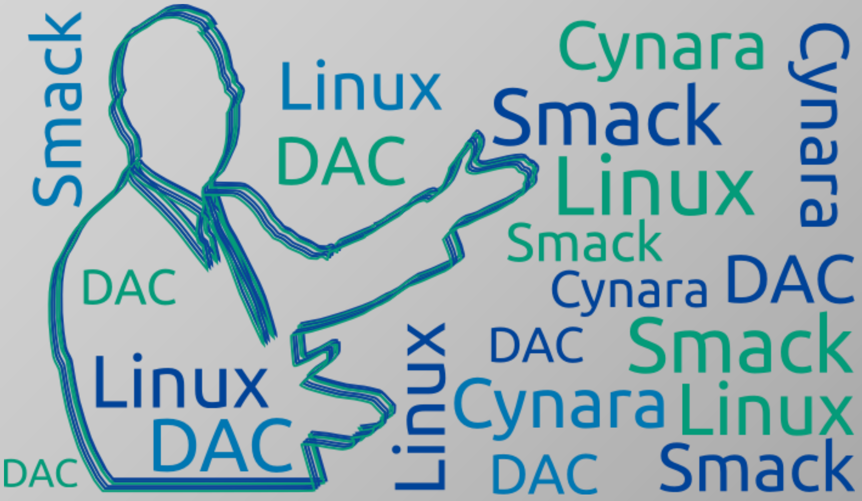


3rd pillar of security: Cynara



Lifecycle of Application

Who manages all of this?



- Security Manager – service managing and configuring all of security modules in operating systems
- Made for Tizen 3.0
- Can be deployed in other Linux distributions

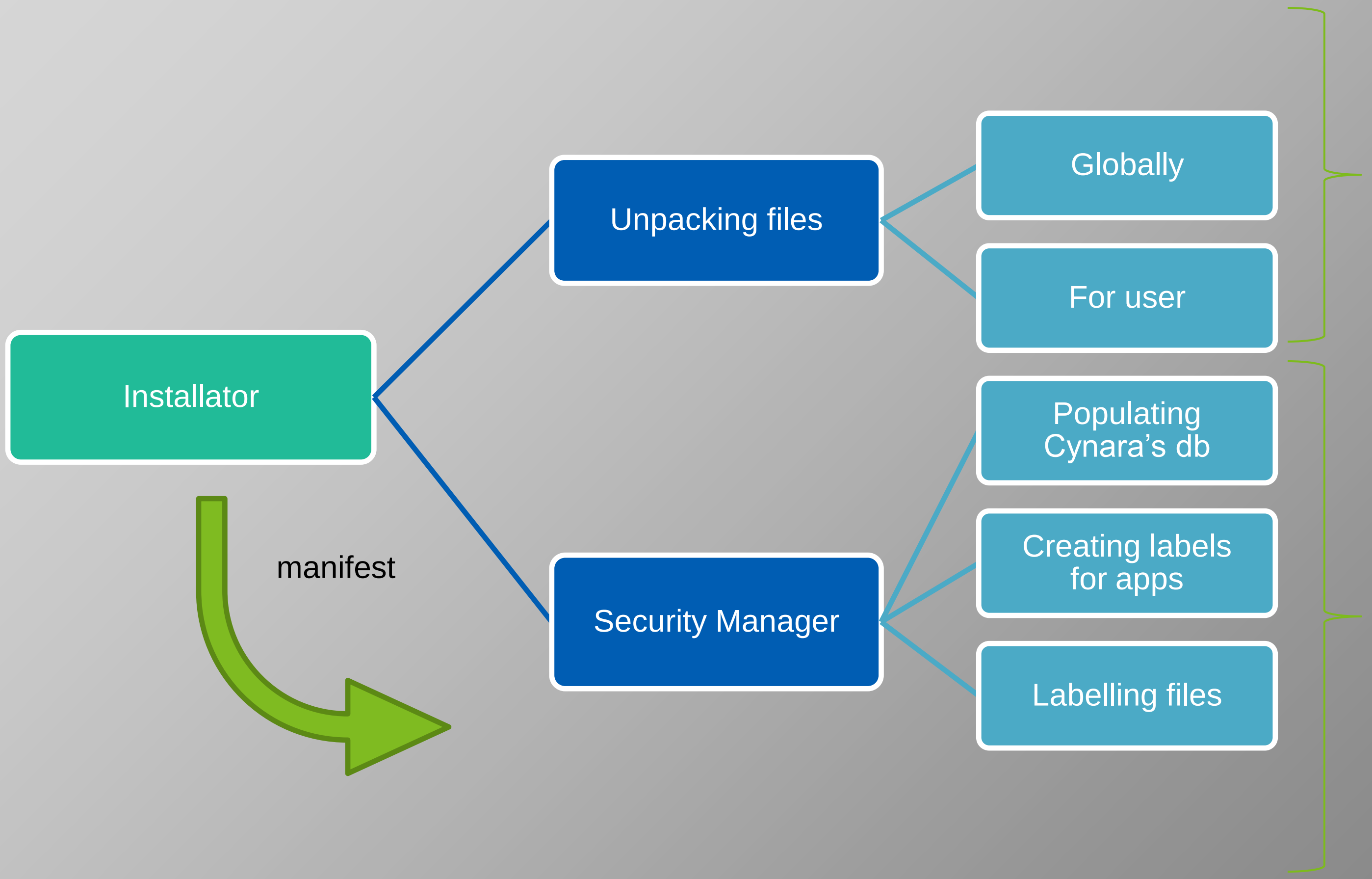
Security Manager

Security Manager is involved in:

- installing applications – populates Cynara's database, creates Smack labels for apps
- launching applications – applies security context (labels, groups) on behalf of launcher
- managing security policies – supports edition of policies by administrator and users (Privacy Manager)
- managing users

(CC) Patrick Breen

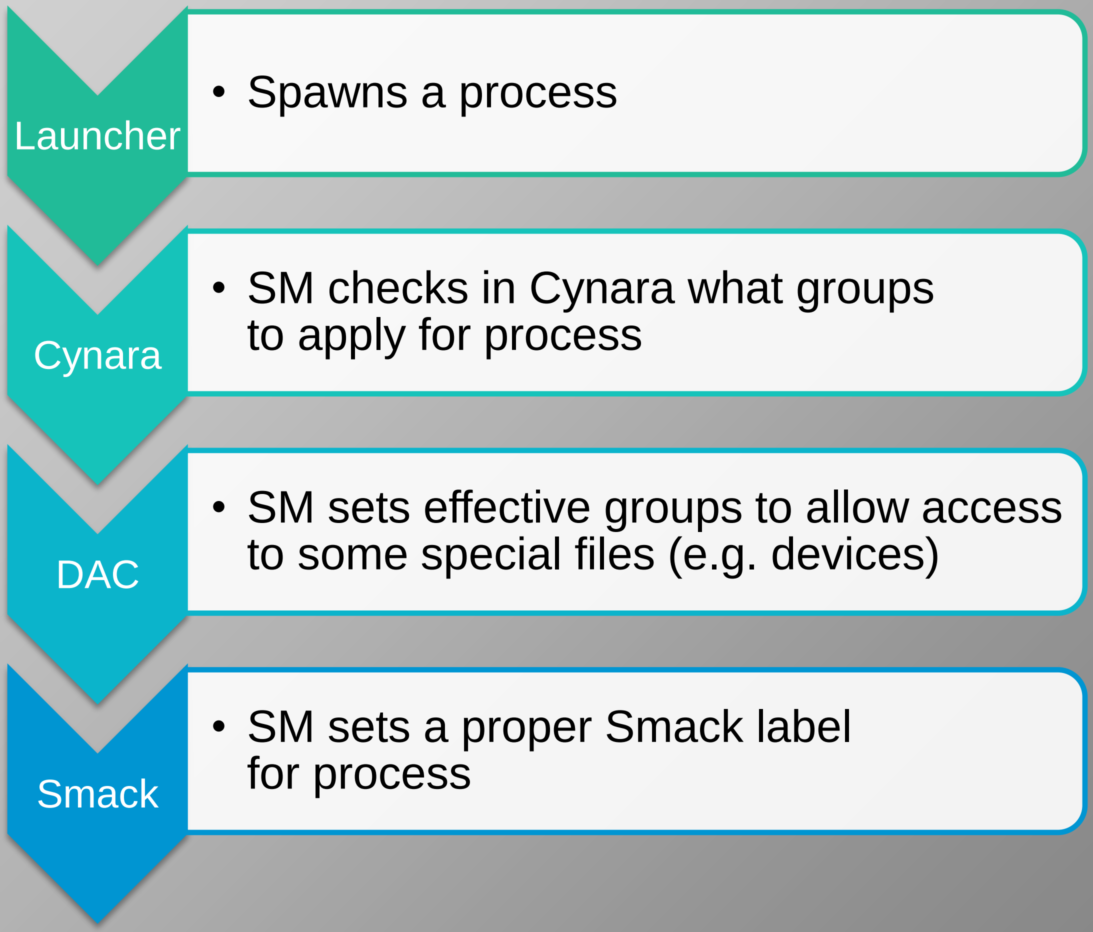
Lifecycle of application: installation



Depends on configuration and privileges

Installator configures application with help from Security Manager

Lifecycle of application: launching



Launcher

- Spawns a process

Cynara

- SM checks in Cynara what groups to apply for process

DAC

- SM sets effective groups to allow access to some special files (e.g. devices)

Smack

- SM sets a proper Smack label for process

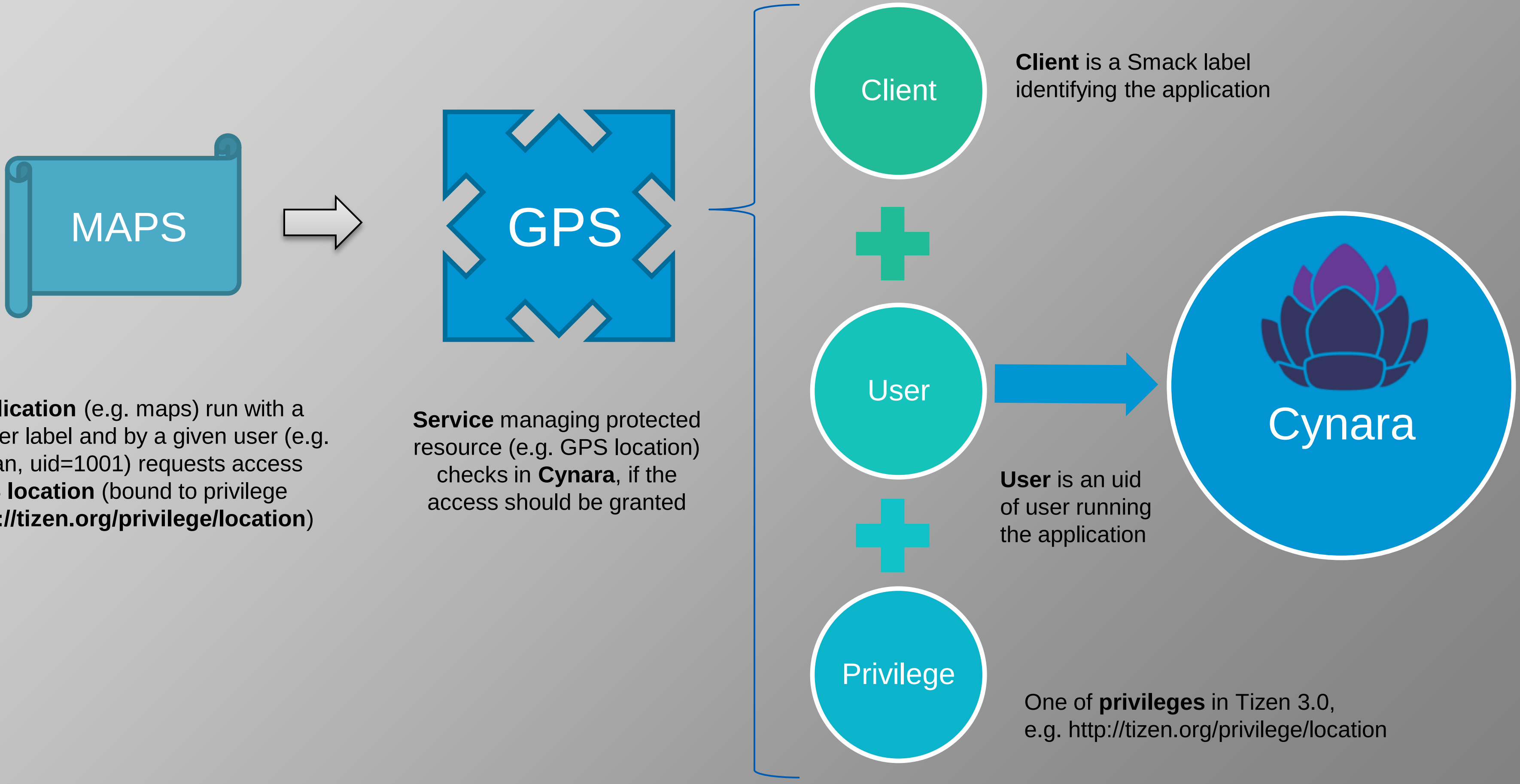
There are some important questions

GPS

Hi Cynara!
Can Maps haz perms to
read location?

Yep, them can haz
dat!

Lifecycle of application: accessing a service



Application (e.g. maps) run with a proper label and by a given user (e.g. Suzan, uid=1001) requests access **GPS location** (bound to privilege **http://tizen.org/privilege/location**)

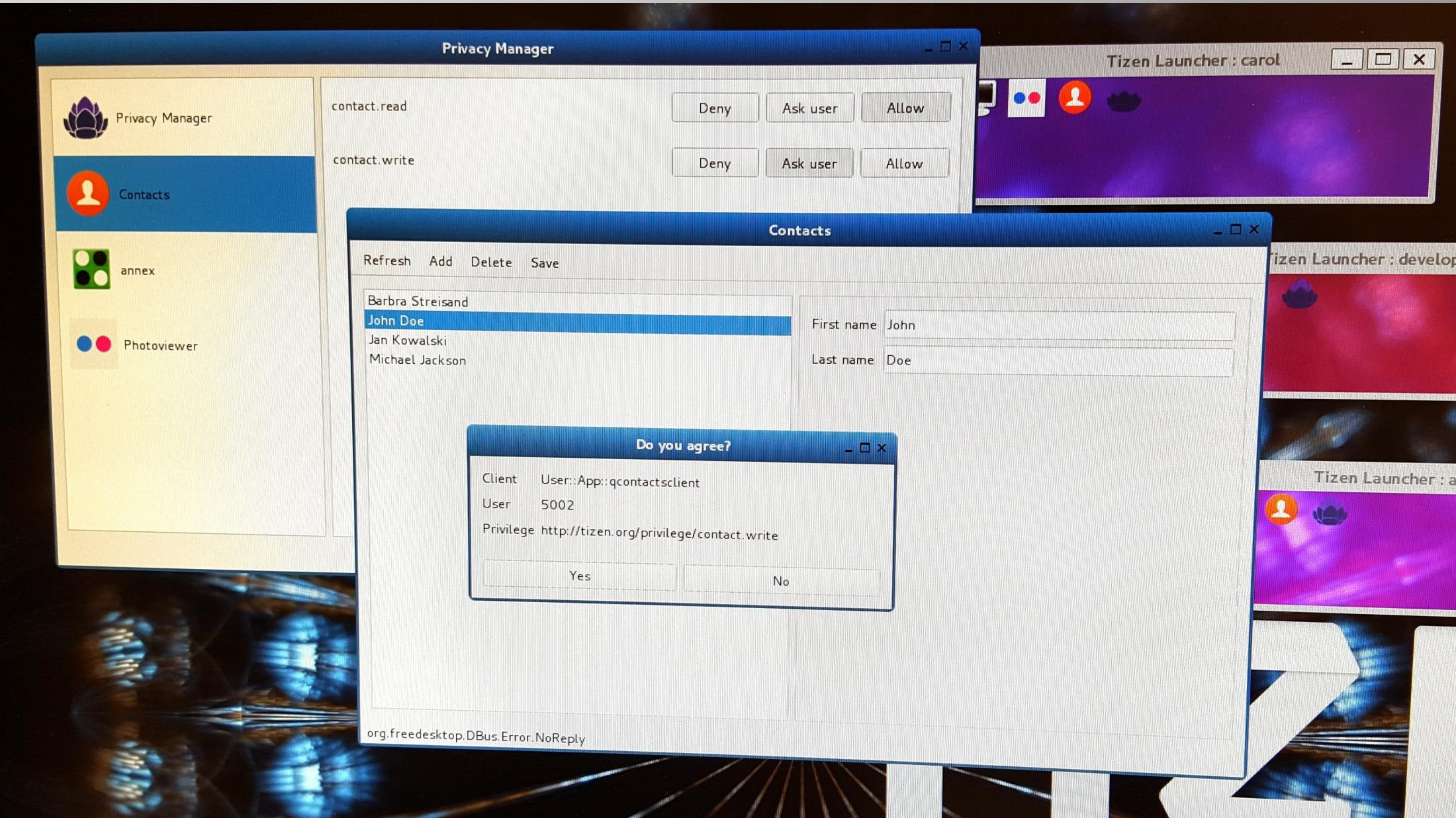
Service managing protected resource (e.g. GPS location) checks in **Cynara**, if the access should be granted

Client is a Smack label identifying the application

User is an uid of user running the application

One of **privileges** in Tizen 3.0, e.g. http://tizen.org/privilege/location

A demo



contact.read Deny Ask user [✓ Allow]

contact.write Deny [✓ Ask user] Allow

Barbra Streisand
John Doe
Jan Kowalski
Michael Jackson

First name John

Last name Doe

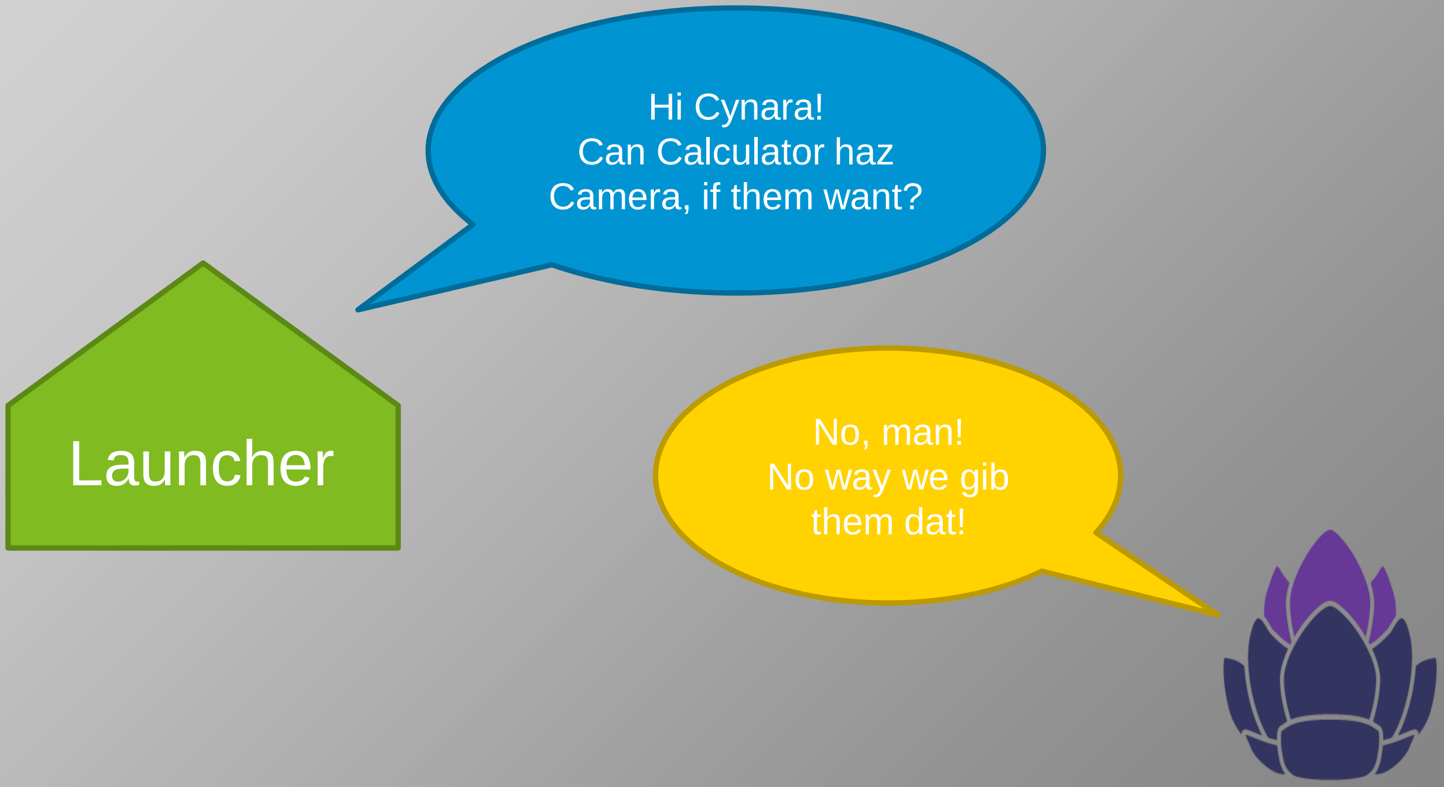
Client User::App::qcontactsclient

User 5002

Privilege http://tizen.org/privilege/contact.write

org.freedesktop.DBus.Error.NoReply

More of important questions…

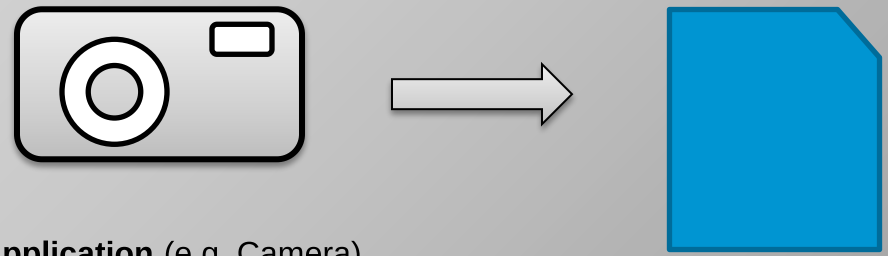


Hi Cynara!
Can Calculator haz
Camera, if them want?

Launcher

No, man!
No way we gib
them dat!

Lifecycle of application: accessing a device



Application (e.g. Camera) run with a proper label and by a given user (e.g. Susan, uid=1001) requests access to device /dev/camera

/dev/camera

Linux checks (DAC) if process belongs to a proper group (e.g. **camera_users**)

Groups are assigned by Security Manager on every launch

Bonuses

Bonuses

- Serving on D-Bus? We’ve got your back
- Nether – networking access control
- nice-lad – auditing
- Vasum – containers

Summary

Summary

- Security of embedded systems and privacy of stored data are very important
- Classic security mechanisms are not enough
- Security must be taken into account from the very beginning
- Security doesn't have to be burdensome for developers

QUESTIONS?

To read

- https://wiki.tizen.org/wiki/Main_Page
- https://wiki.tizen.org/wiki/Security/Overview
- https://wiki.tizen.org/wiki/Security:Cynara
- https://wiki.tizen.org/wiki/Security:nice-lad

To read

- https://github.com/Samsung/security-manager
- https://github.com/Samsung/nether
- https://github.com/Samsung/nice-lad
- https://github.com/Samsung/vasum
- https://github.com/Samsung/cynara

Pictures used

- https://www.flickr.com/photos/elektronikkbransjen/15523115208/
- https://www.flickr.com/photos/intelfreepress/8047838494/
- https://www.flickr.com/photos/saschamuesse/15563157851/
- https://wiki.tizen.org/wiki/File:IVISimulator2.png
- http://en.wikipedia.org/wiki/Tux#/media/File:Tux.png
- http://en.wikipedia.org/wiki/Smack_(software)#/media/File:Smack-tux.svg

Thanks for listening