Ubuntu Application Confinement

Or: How I learned to stop worrying and trust application developers

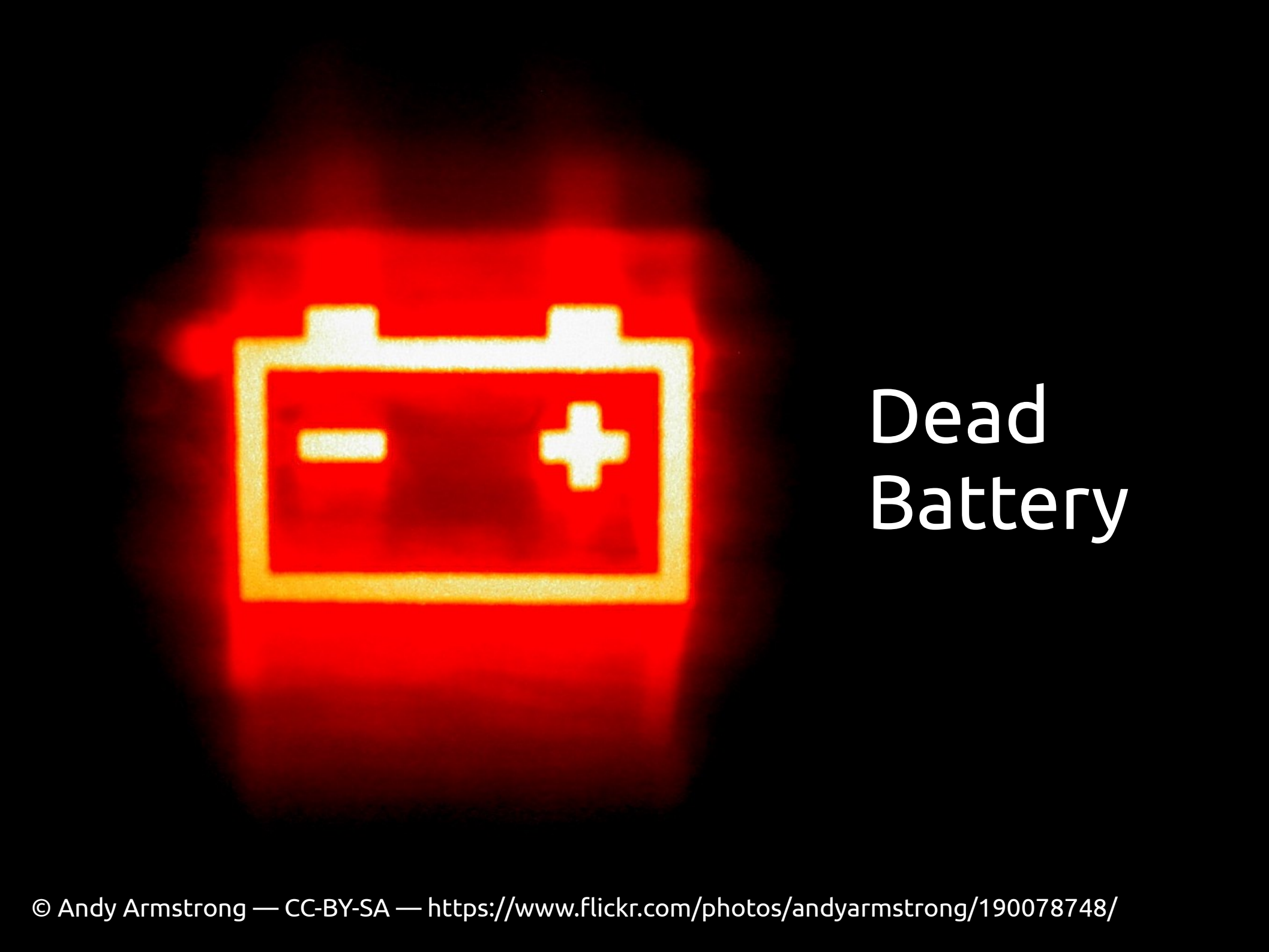
Ted Gould
ted@canonical.com
@tedjgould
SMU
3 Sept 2014

“I'm more worried about Murphy than I am Machievilli”

— Michi Henning


Ideal
Cracker

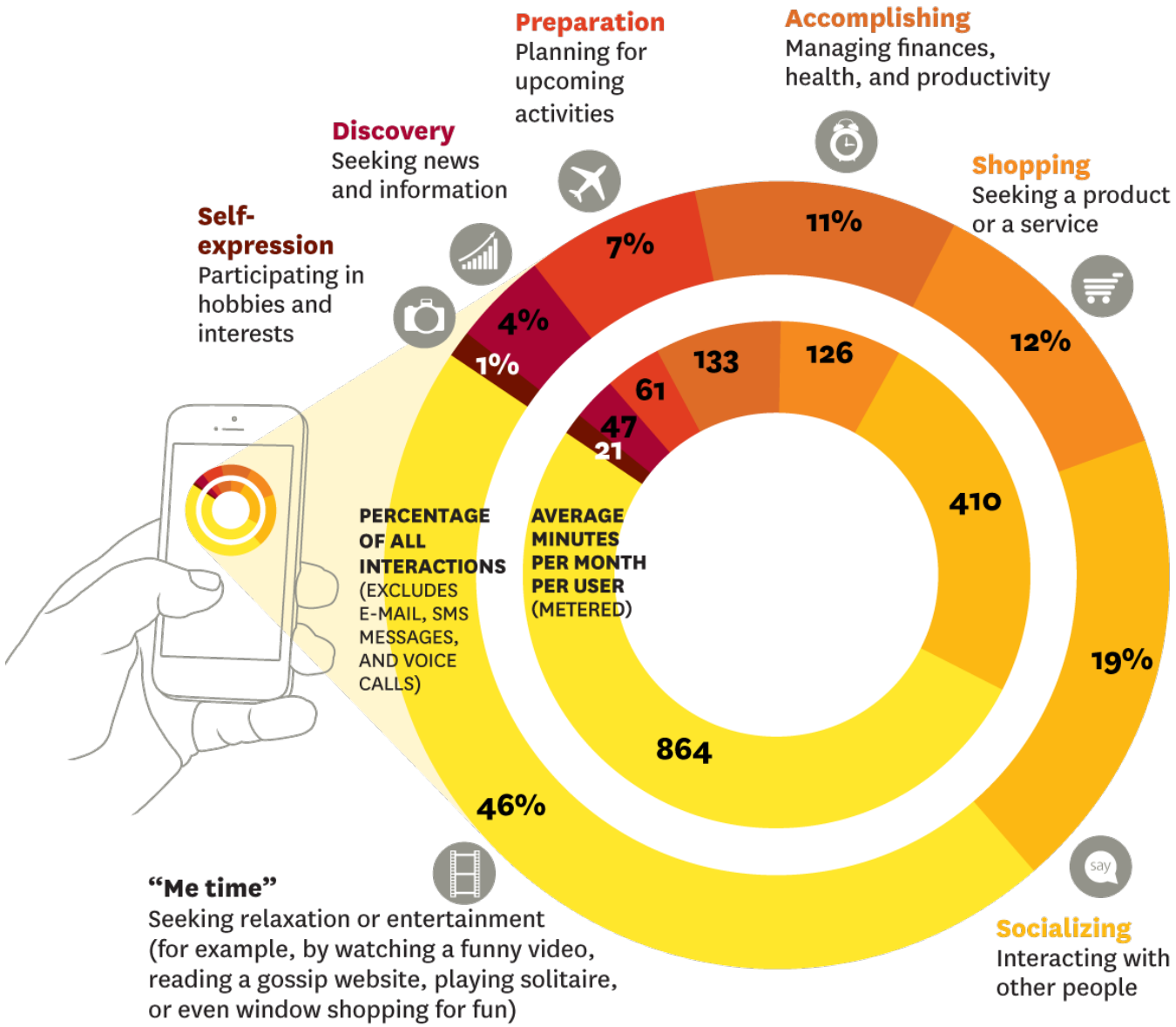

Diminished User Experience
CORE TEMP



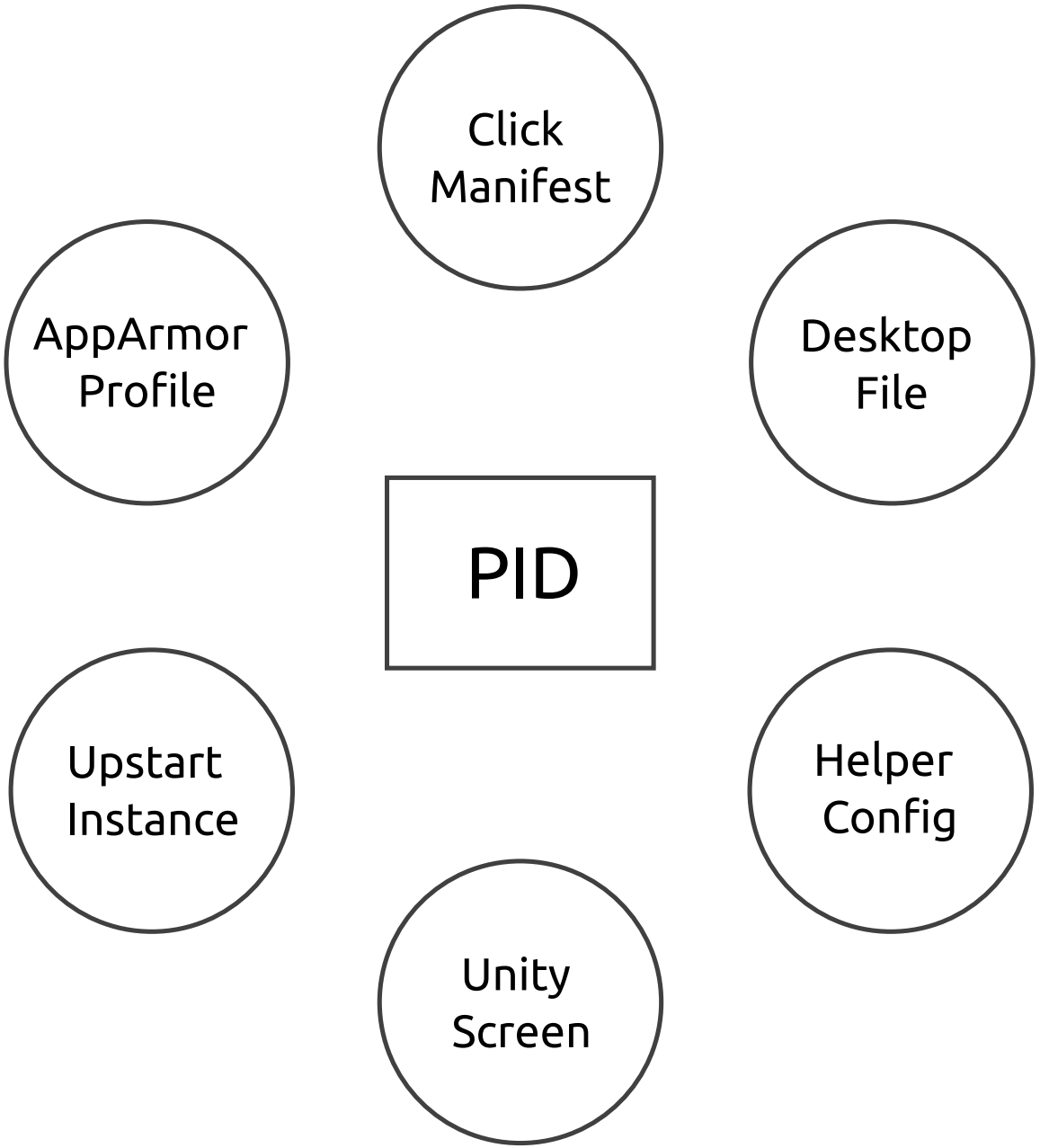
Data Protection

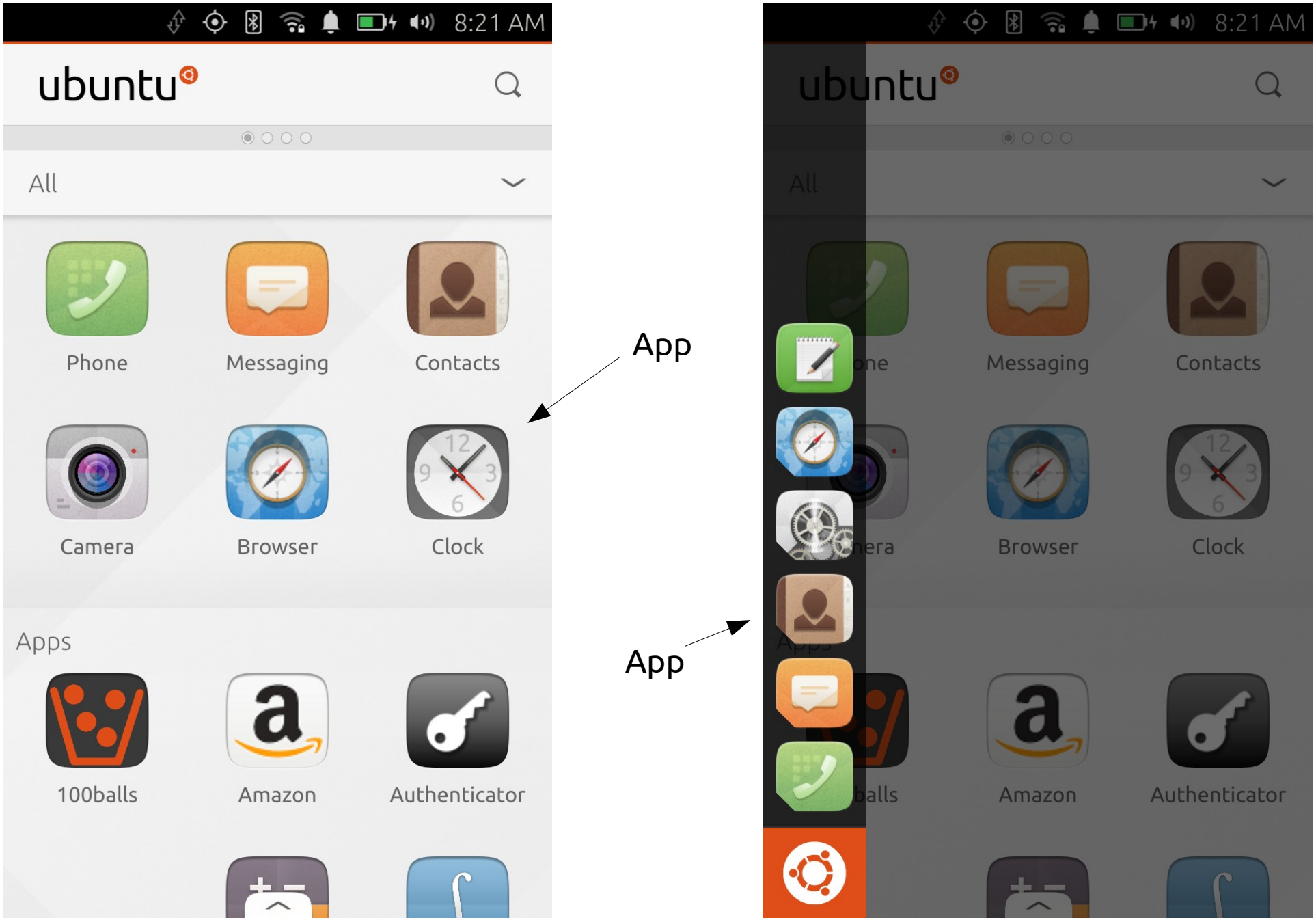
Physical Destruction

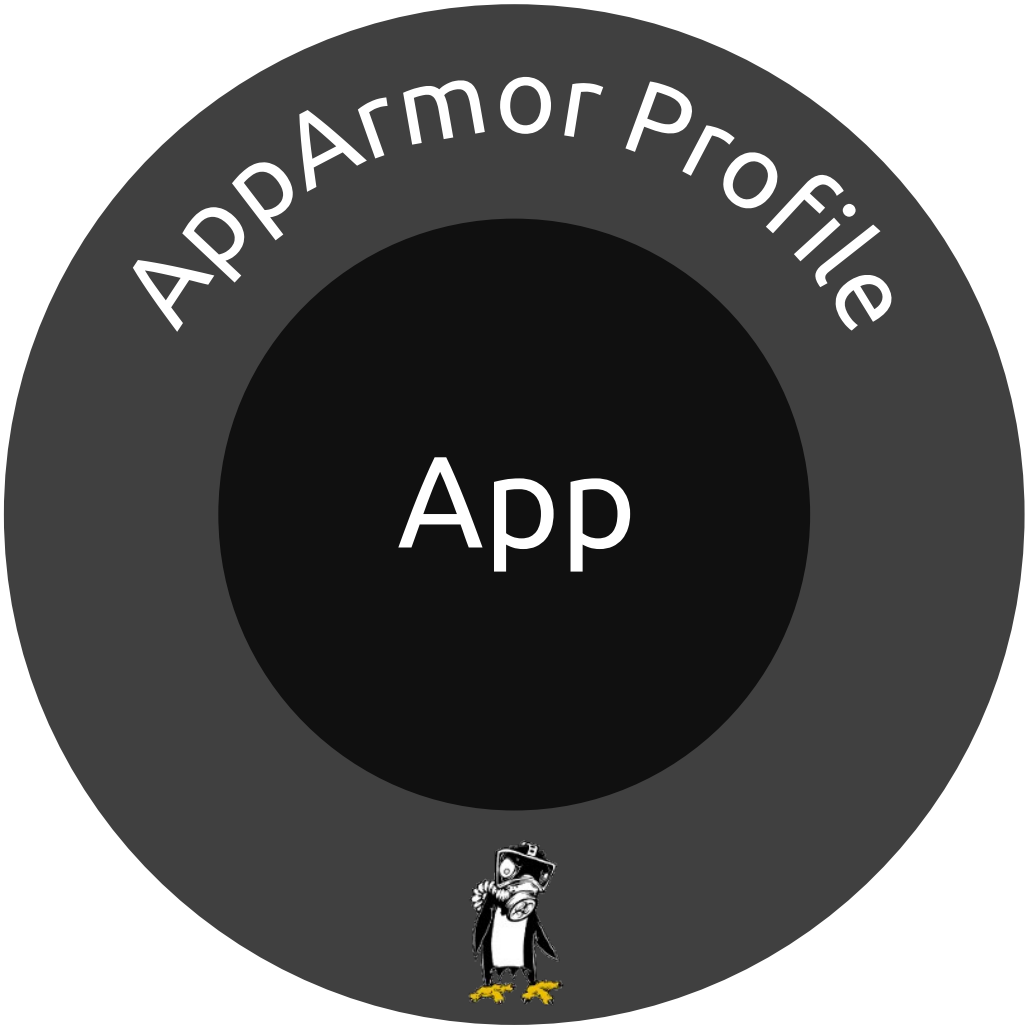
Phone Usage

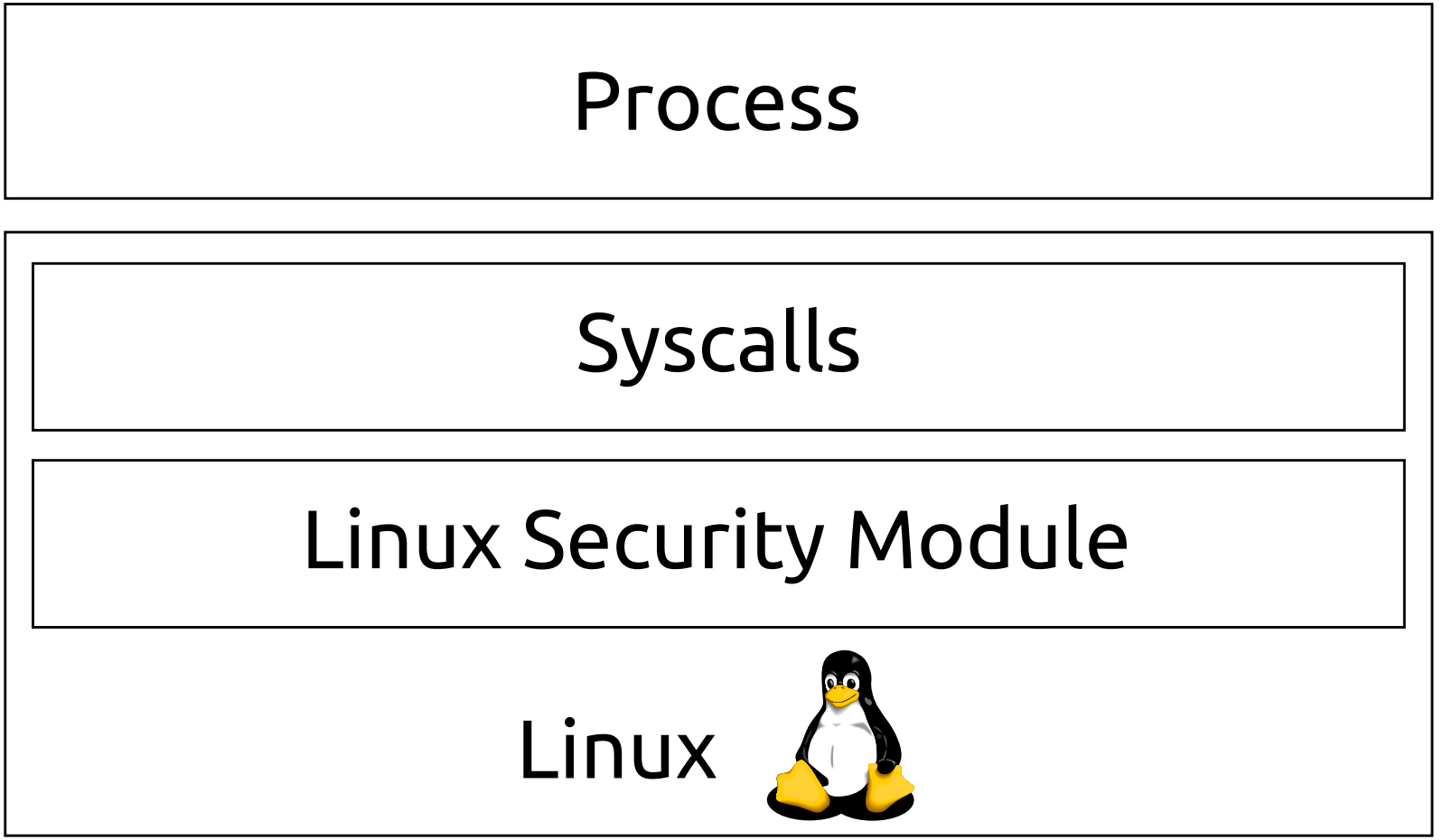


http://hbr.org/2013/01/how-people-really-use-mobile/


Click
Manifest
AppArmor
Profile
Desktop
File
PID
Upstart
Instance
Helper
Config
Unity
Screen


8:21 AM
ubuntu
All
Phone
Messaging
Contacts
Camera
Browser
Clock
Apps
100balls
Amazon
Authenticator
App
App

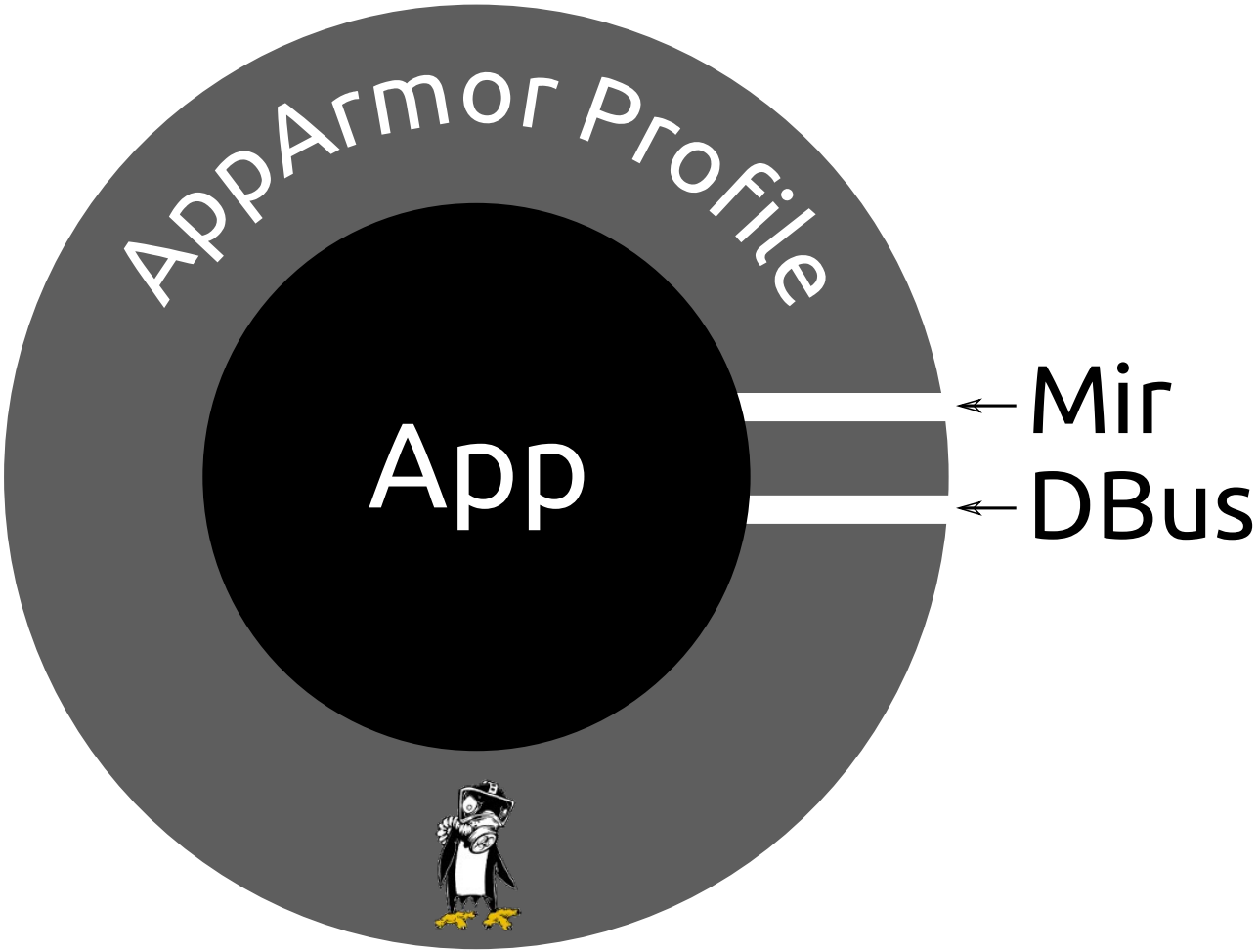

AppArmor Profile
App

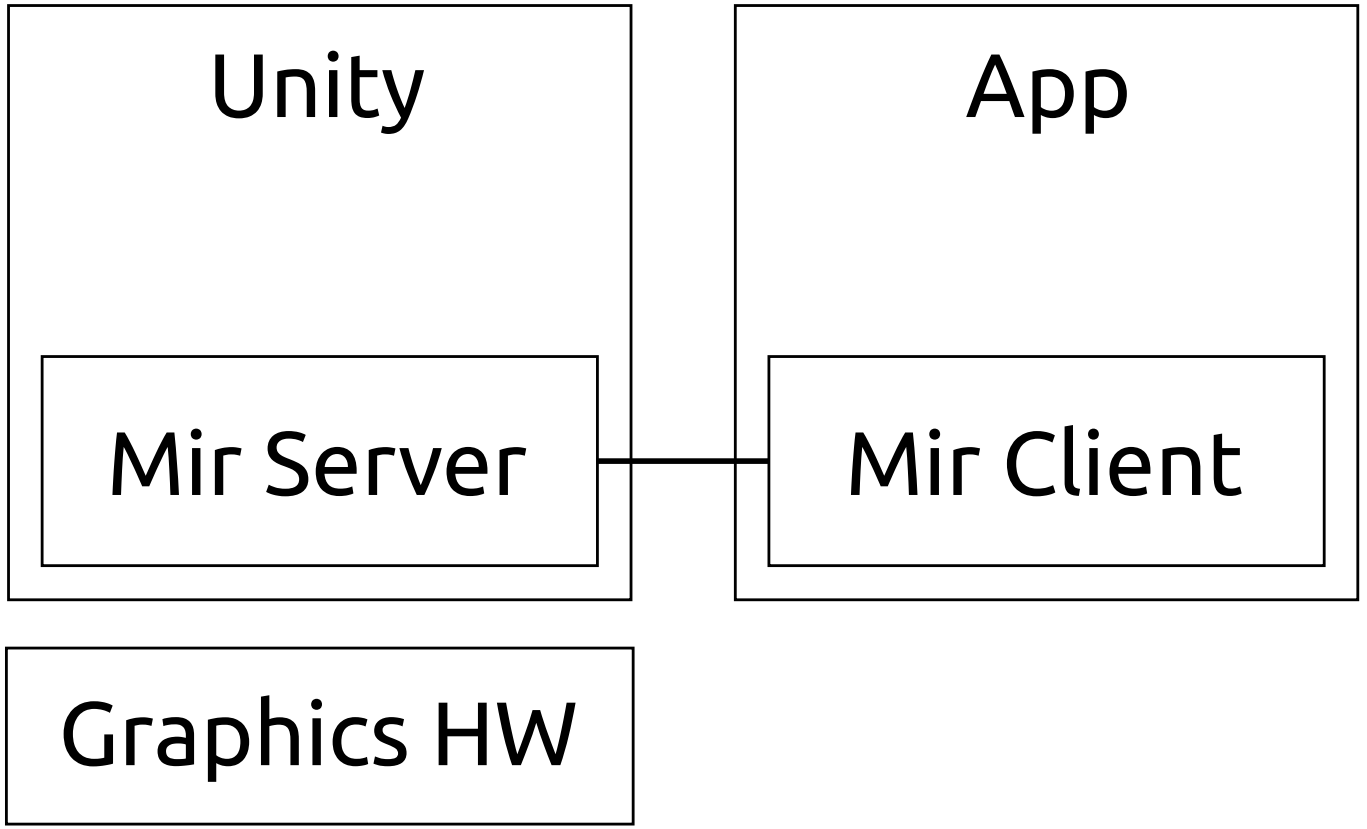

Process
Syscalls
Linux Security Module
Linux

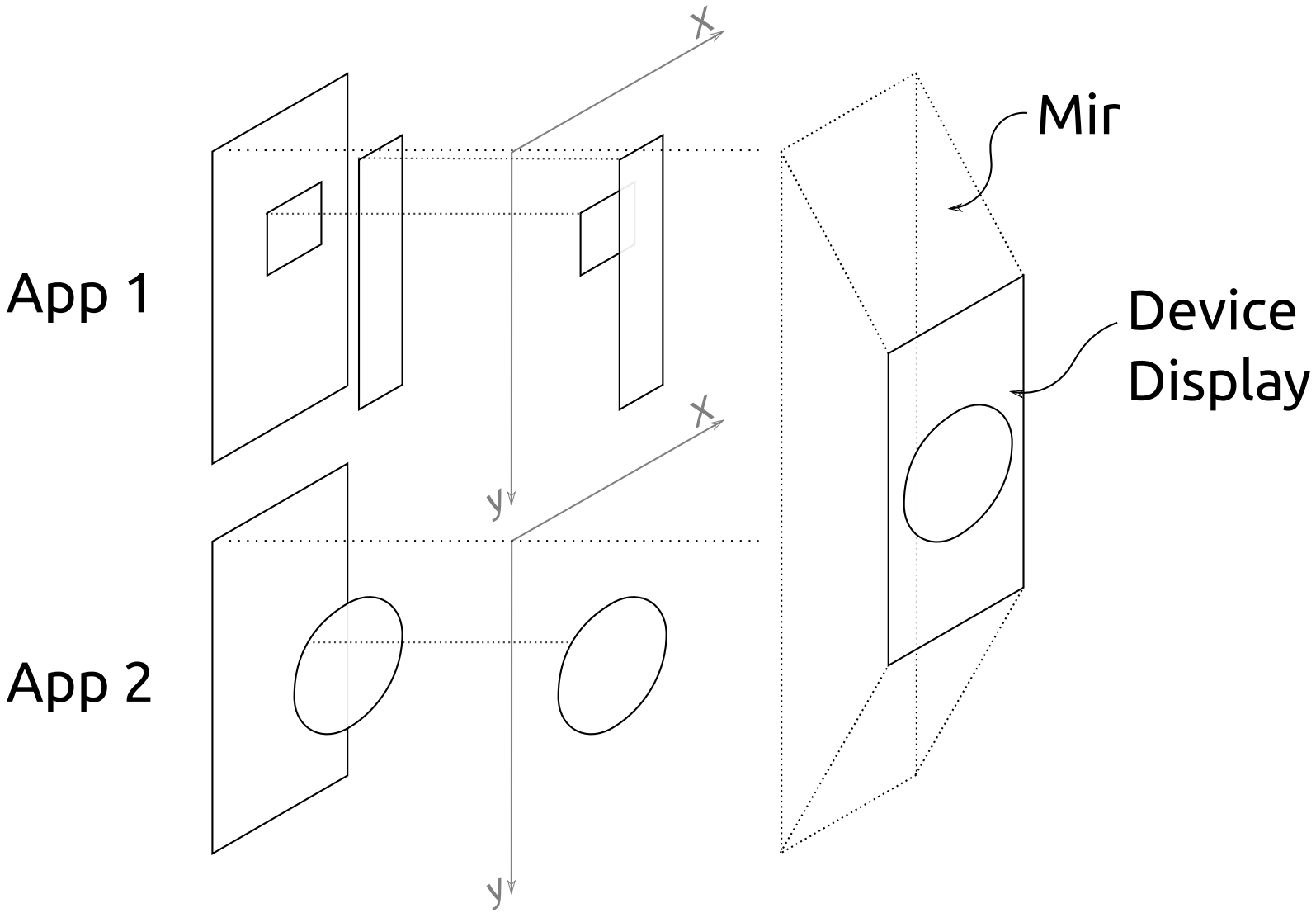
App Writable Area
~/.cache/$(pkg)
~/.local/share/$(pkg)
~/.config/$(pkg)

App Readable Area
/usr/share/icons/
/bin/sh
/usr/bin/qmlscene

App Restricted Area
~/.cache/$(other pkg)
~/.local/share/address-book
~/Documents/

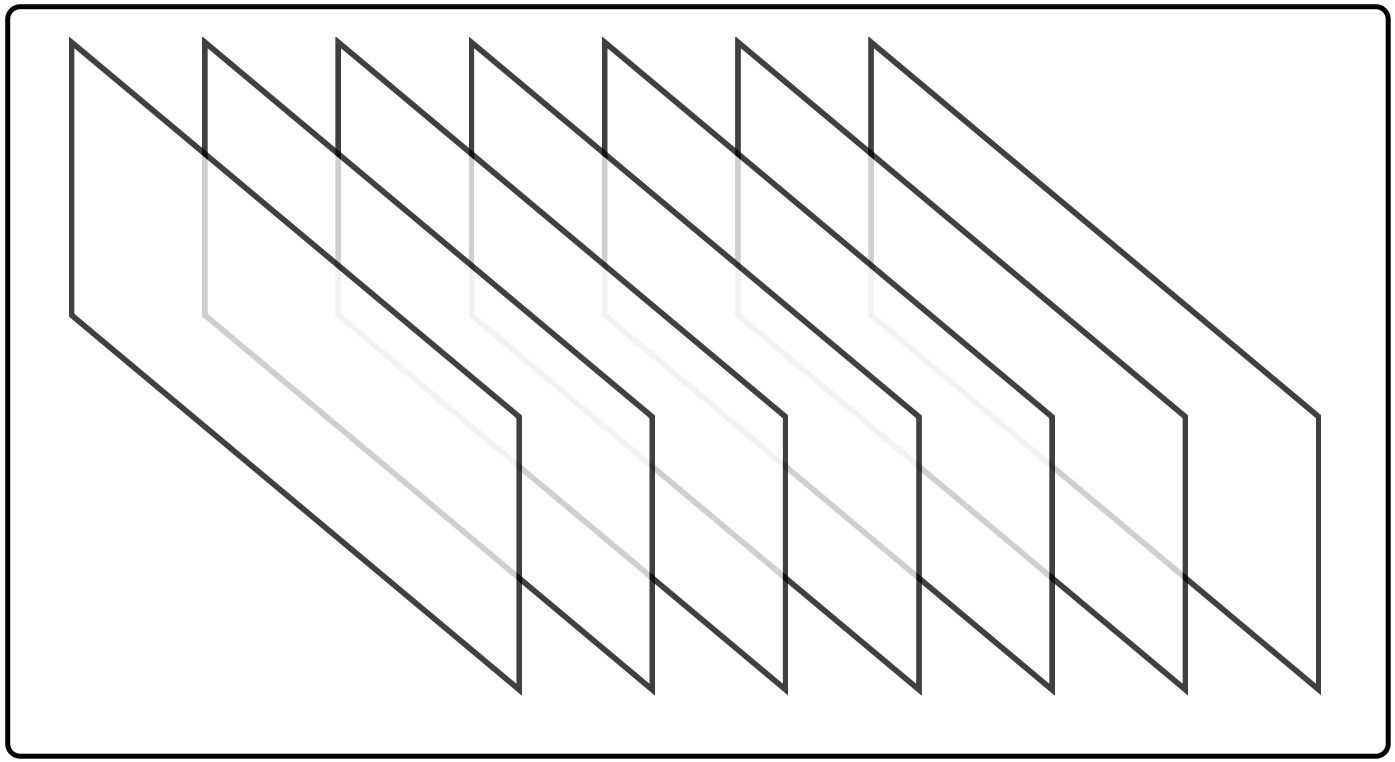

AppArmor Profile
App
Mir
DBus


Unity
App
Mir Server
Mir Client
Graphics HW

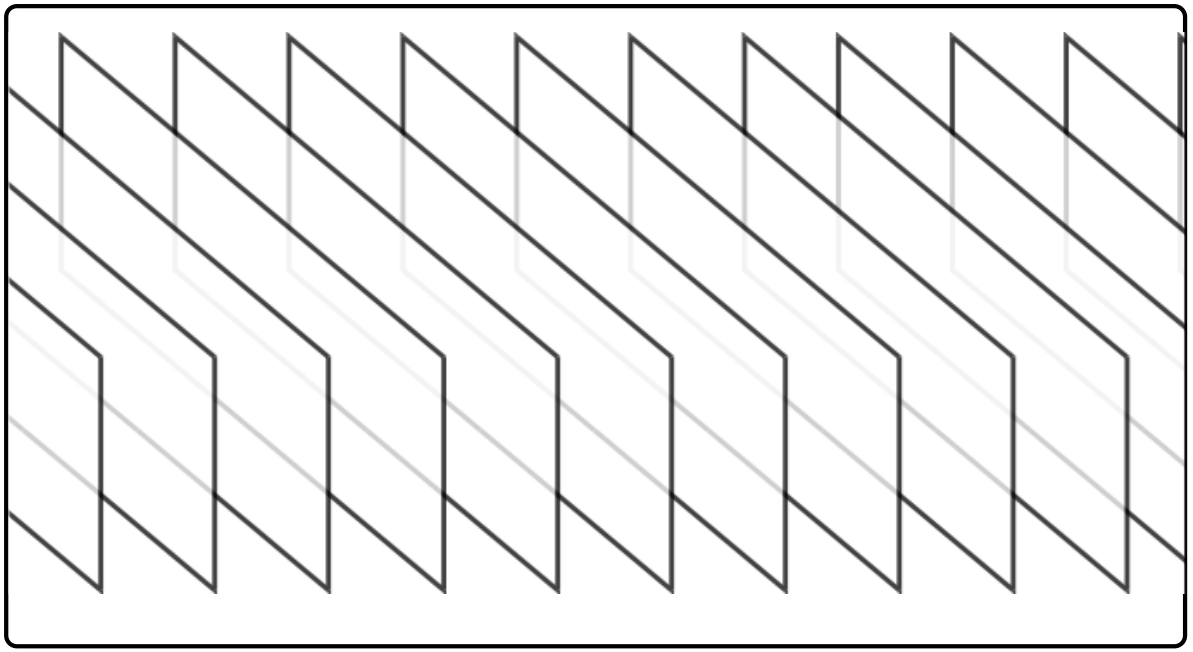

App 1
App 2
x
y
x
y
Mir
Device
Display

Application Switcher

Presentation Application Switcher



Infinite App Illusion

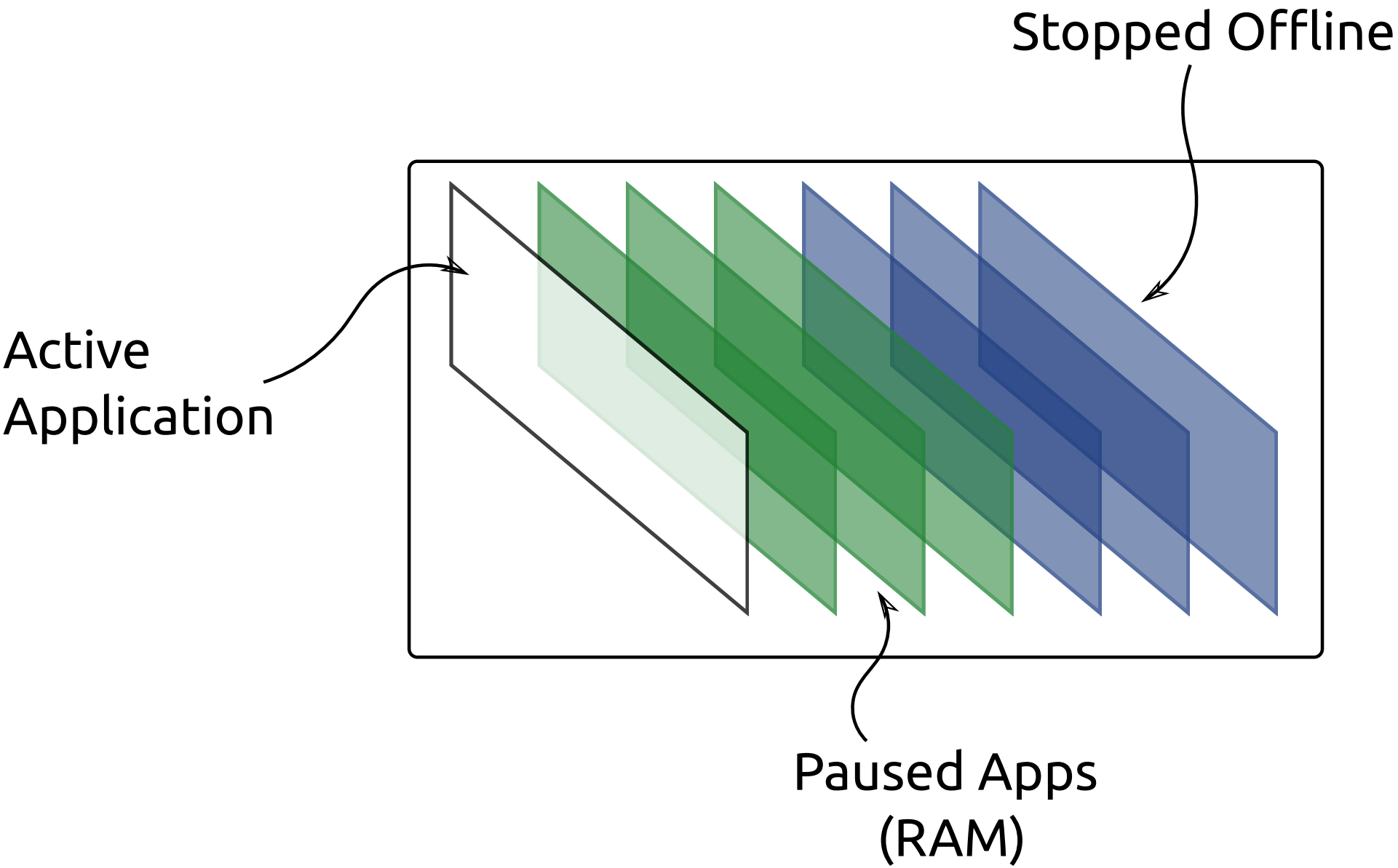


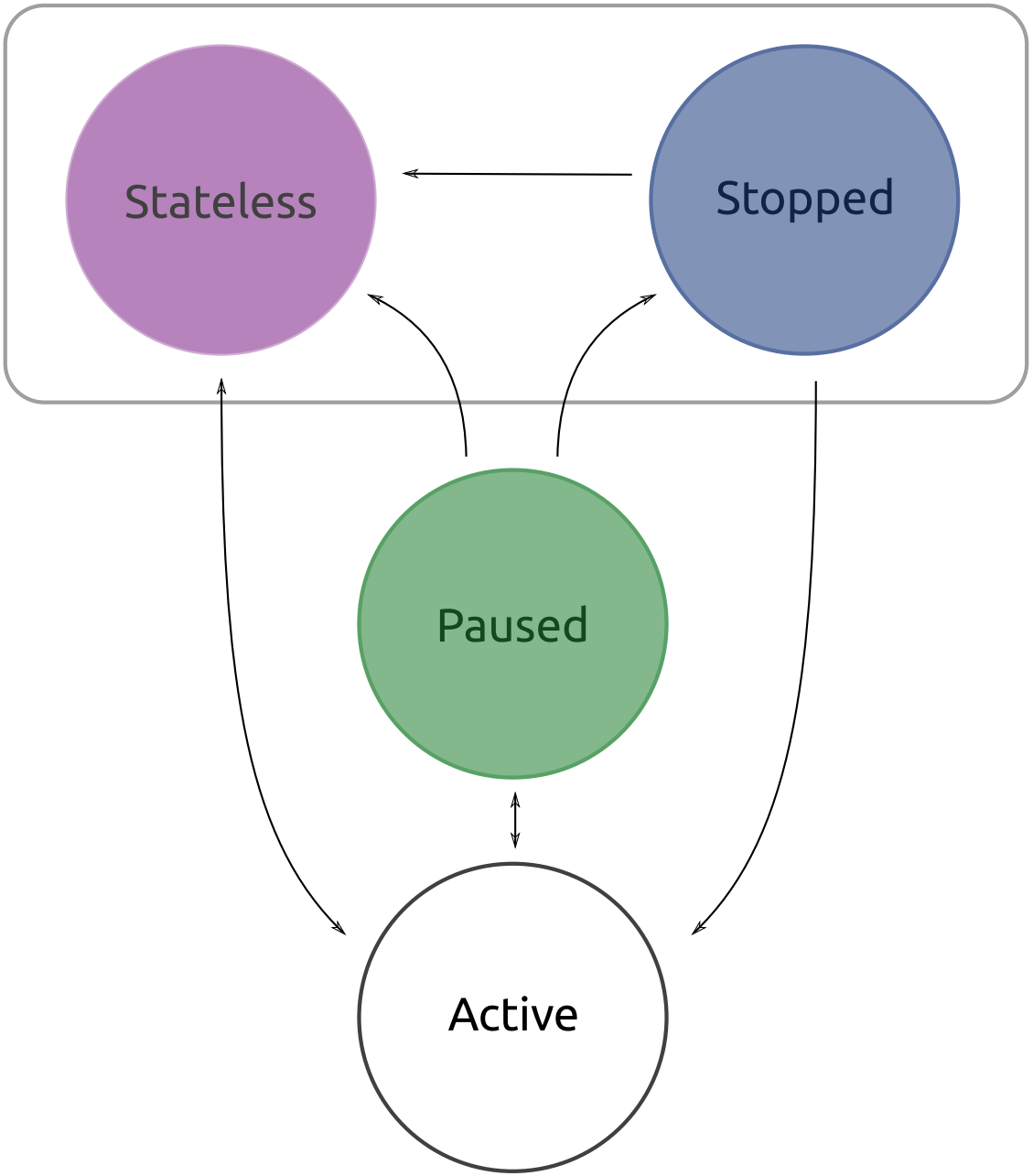
Technical

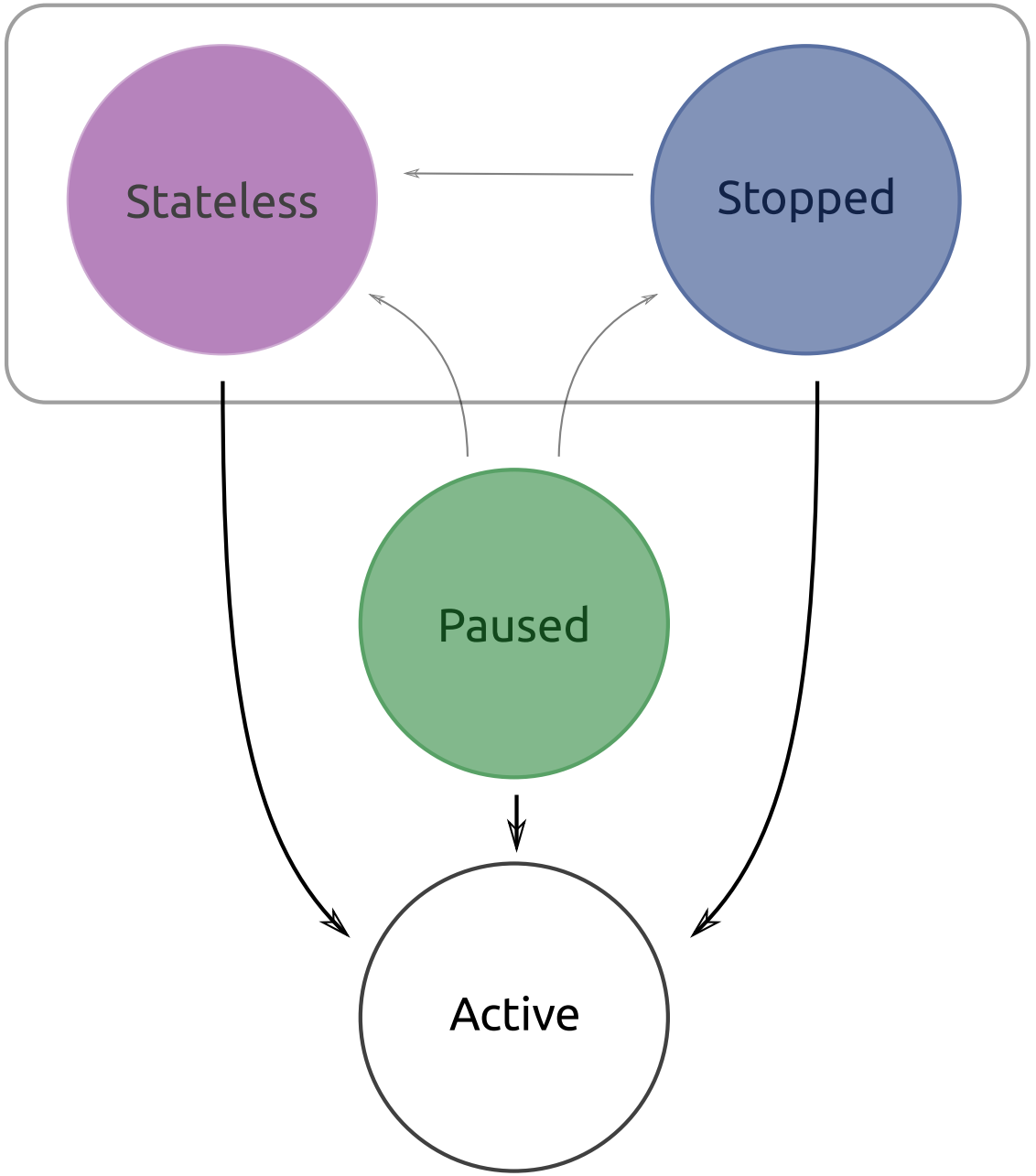
1 GB RAM
1 GHz Quad Core

User

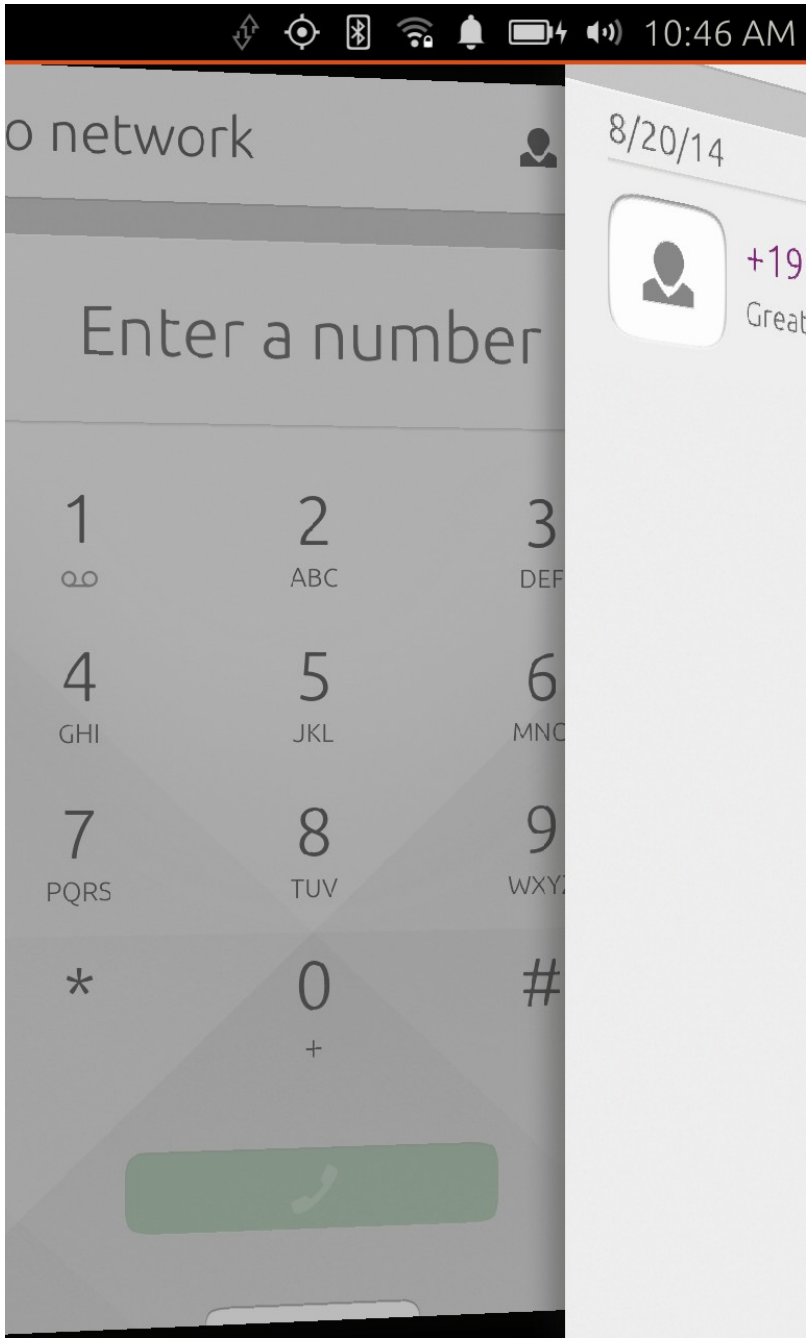
How many
apps can I run?

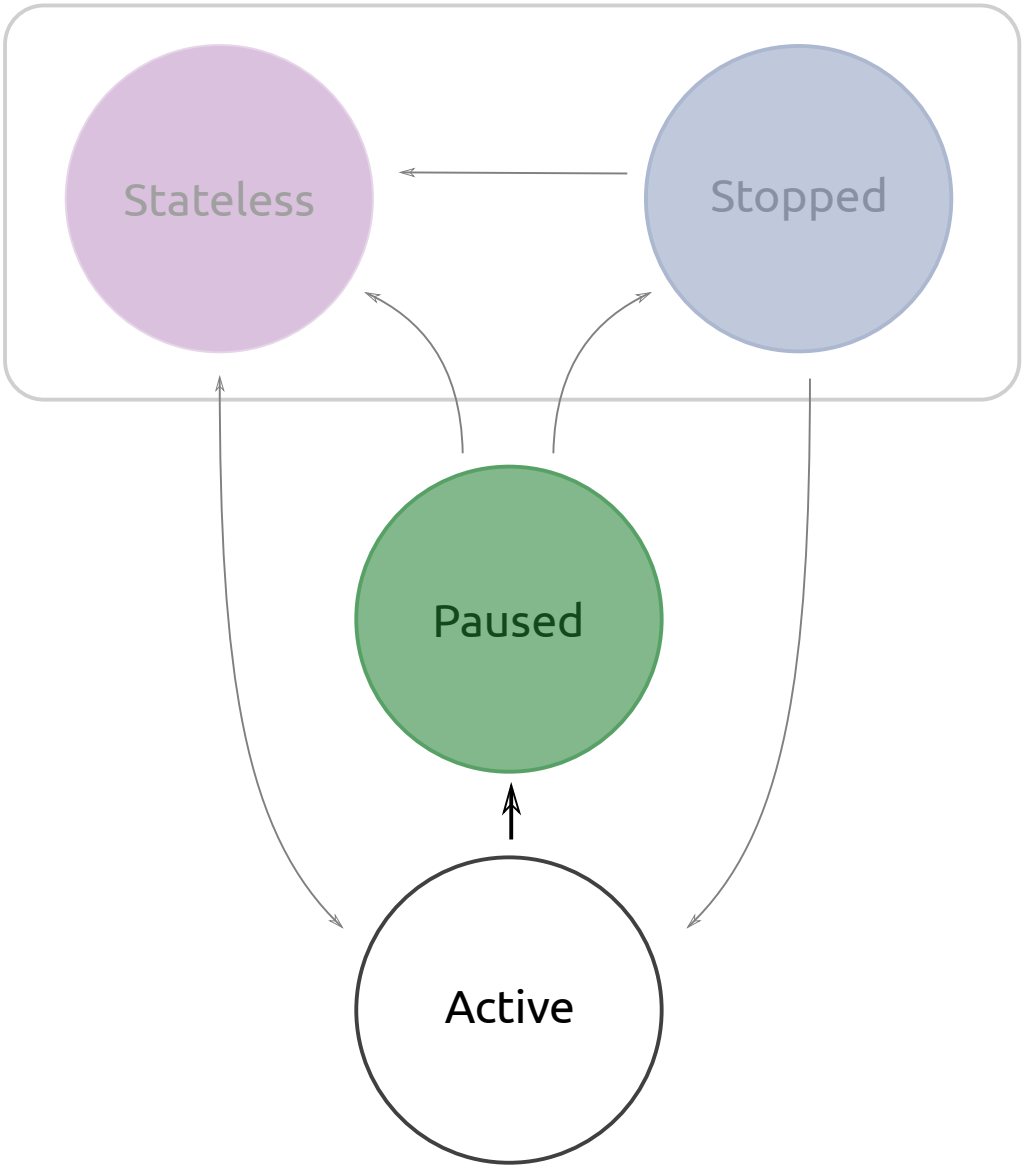

Stopped Offline
Active
Application
Paused Apps
(RAM)

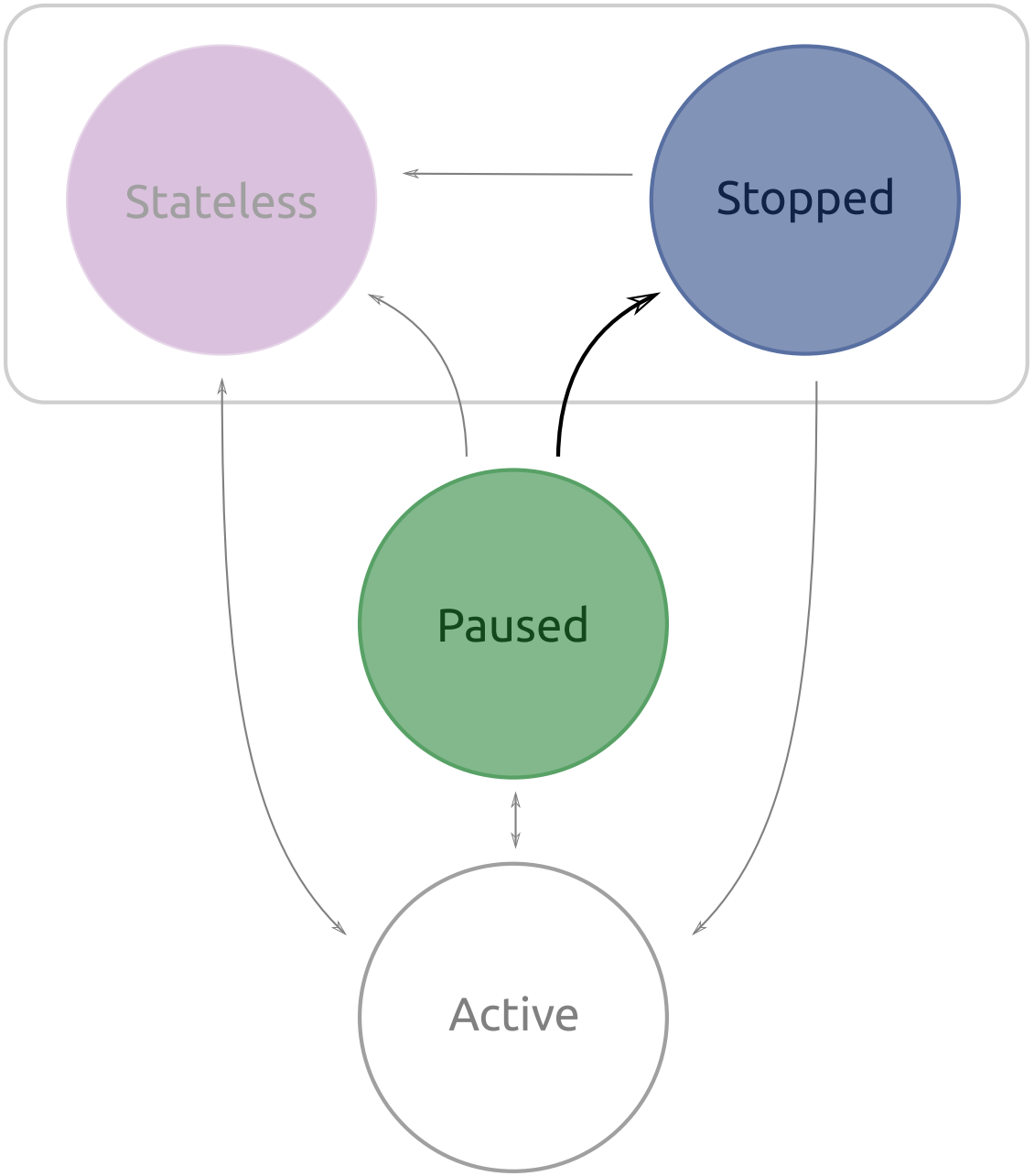

Stateless
Stopped
Paused
Active



User Interaction Only!!!

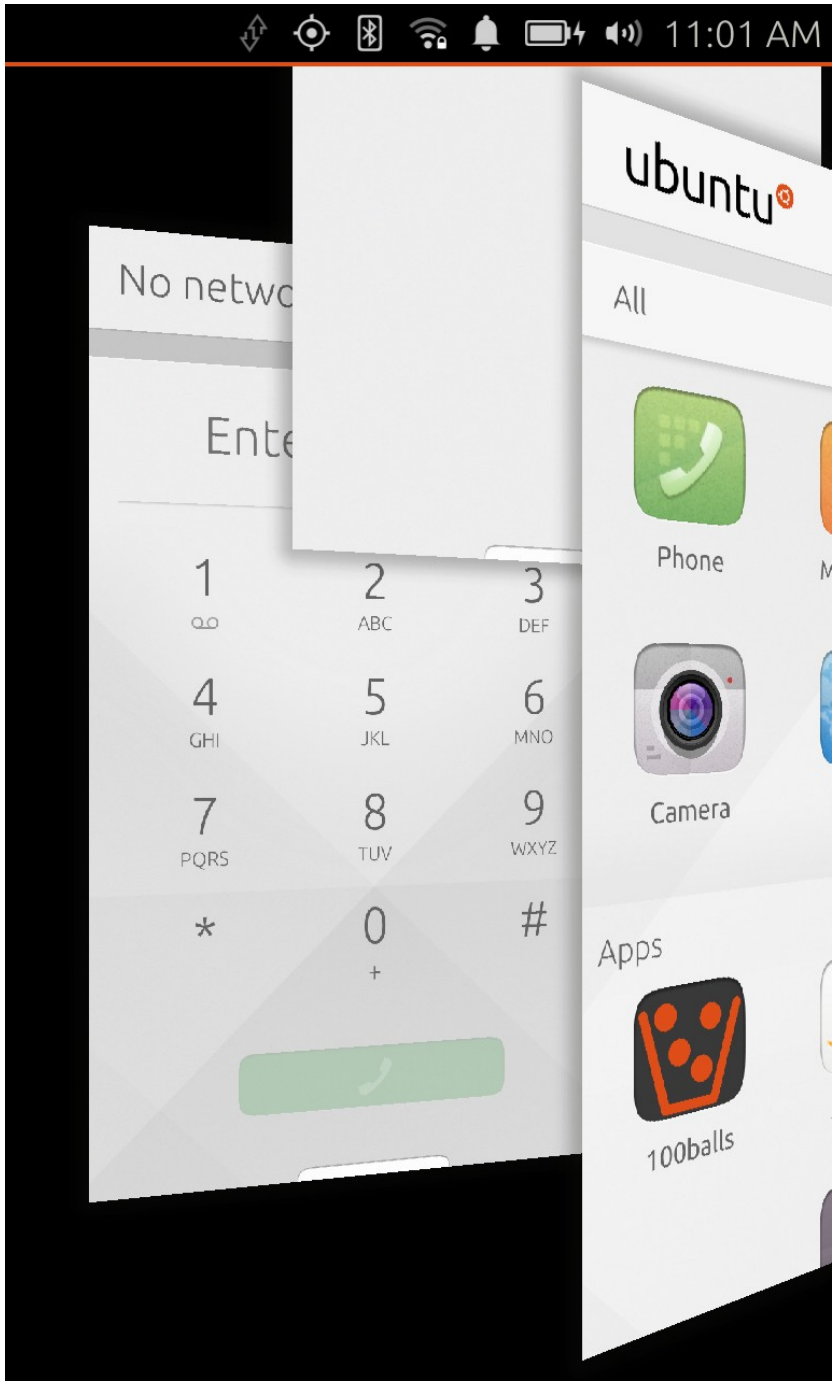

10:46 AM
o network
Enter a number
8/20/14
+19
Great
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0 +
#

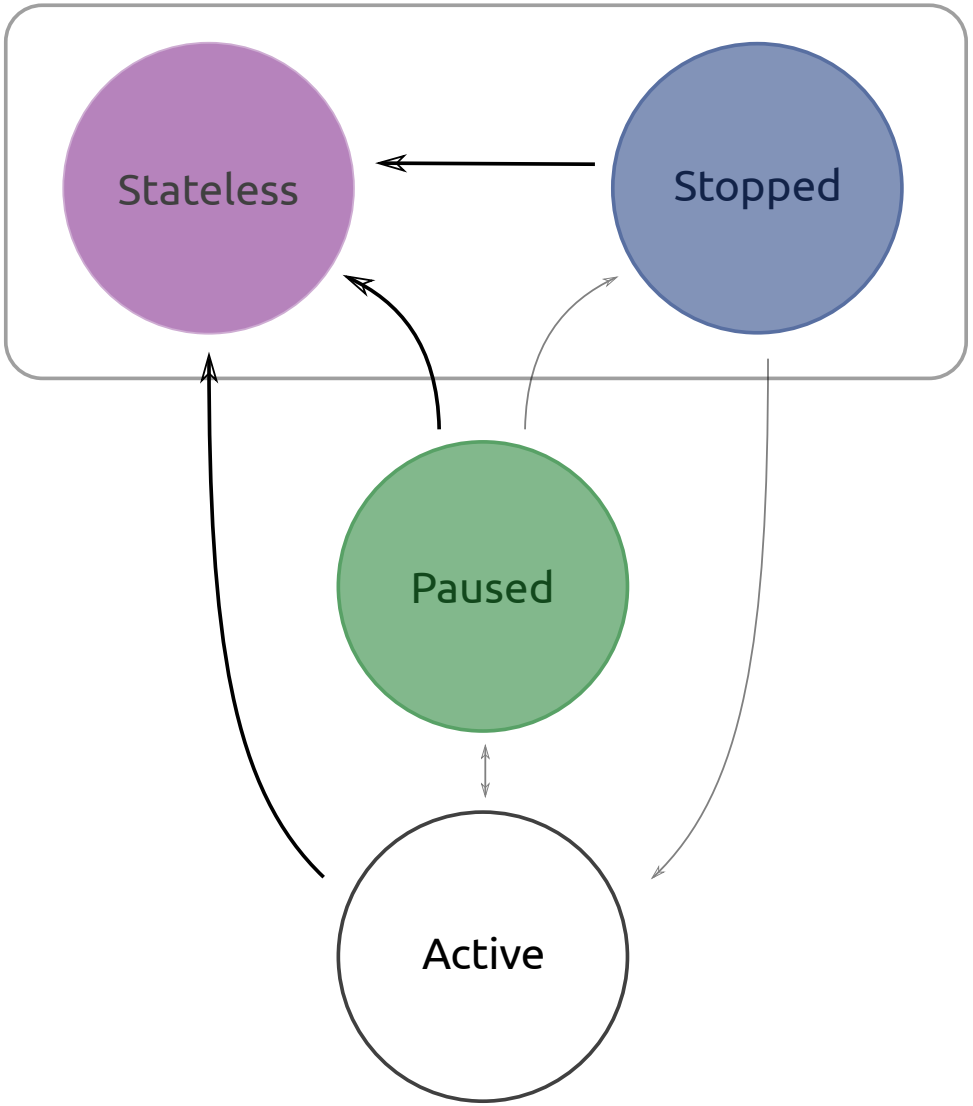

Stateless
Stopped
Paused
Active

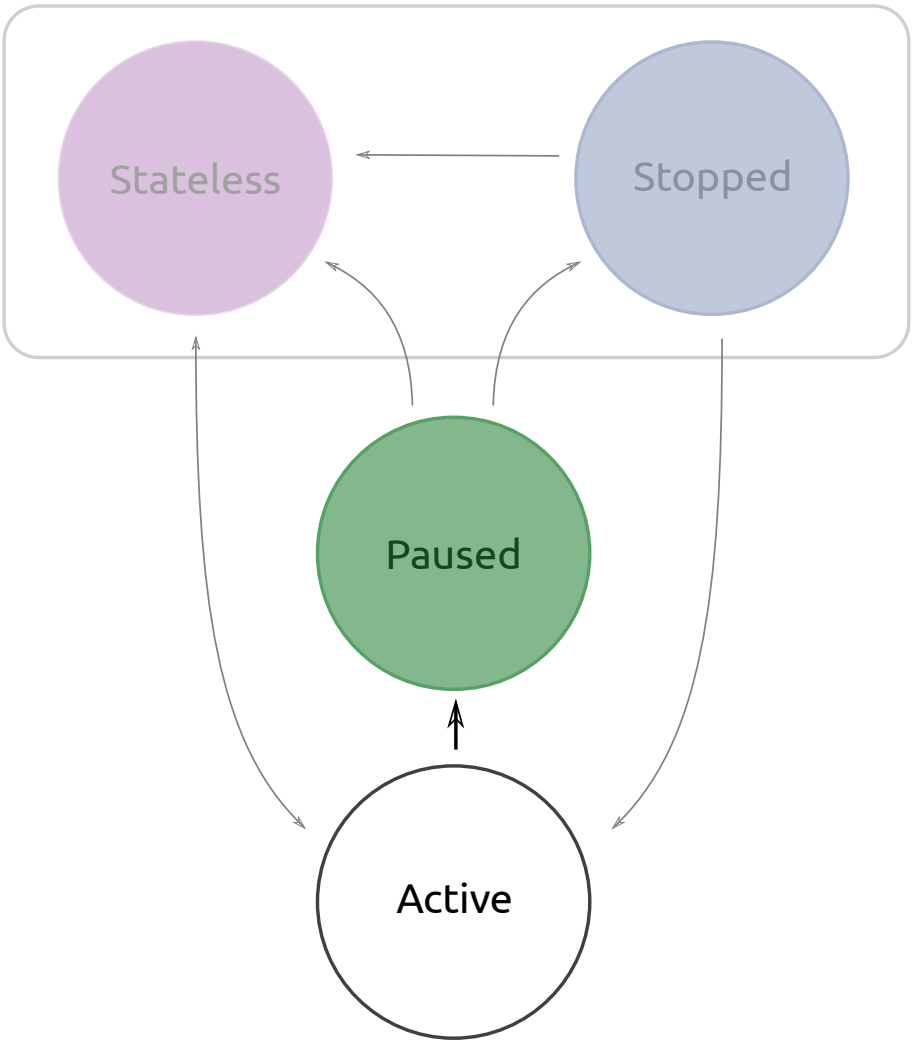


Linux Kernel OOM Killer

(want to include graphics resources in the future)

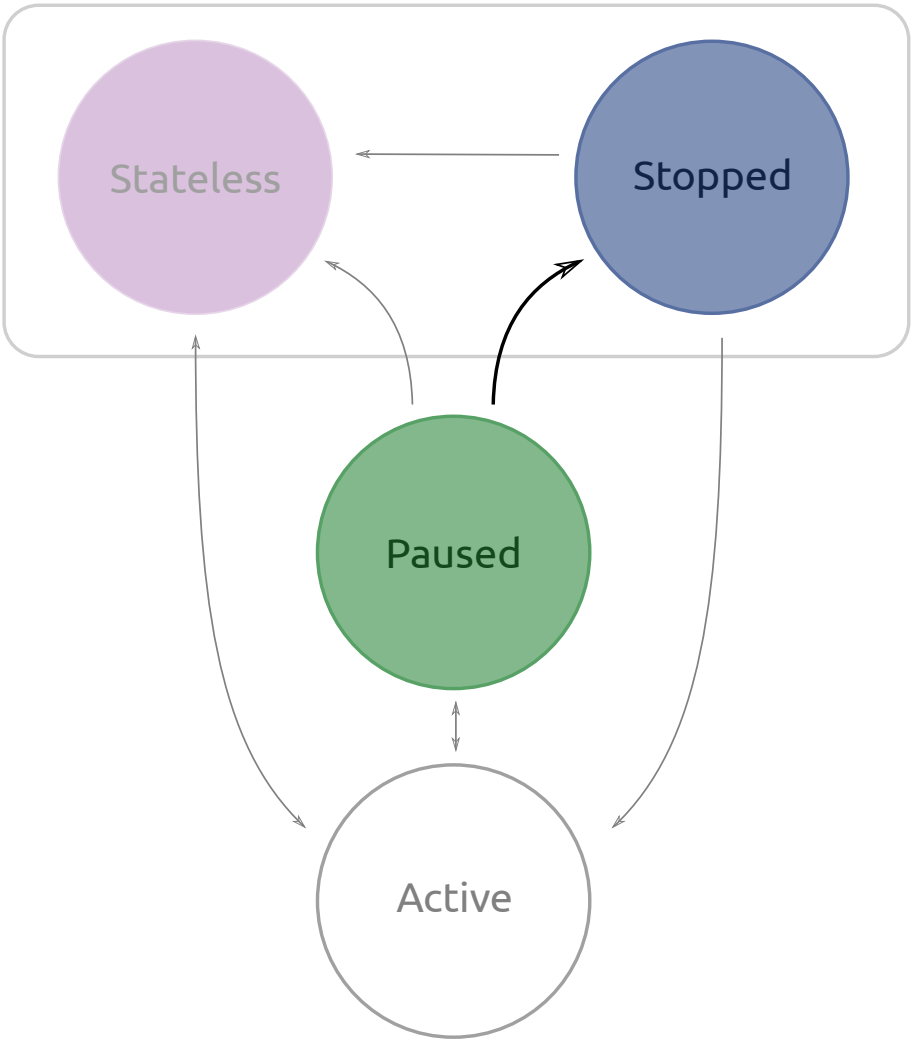

11:01 AM
ubuntu
All
Phone
Camera
Apps
100balls
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0 +
#


Stateless
Stopped
Paused
Active



What happens:

- App is asked to save state
- Graphic buffers grabbed for screenshot
- Timeout, then all processes are sent SIGSTOP



What happens:

- NOTHING!

Positive:

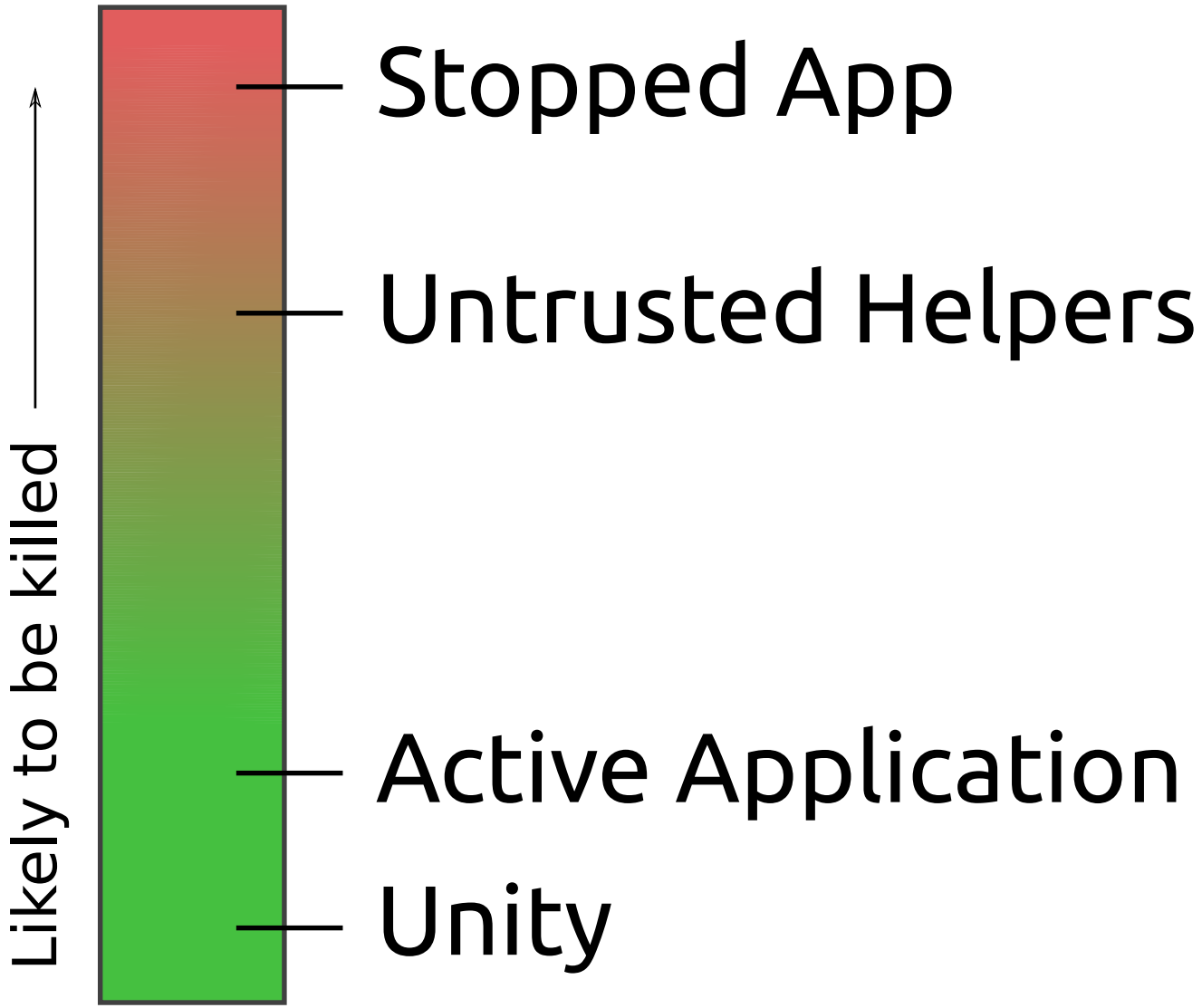
Ask to save state nicely via life cycle

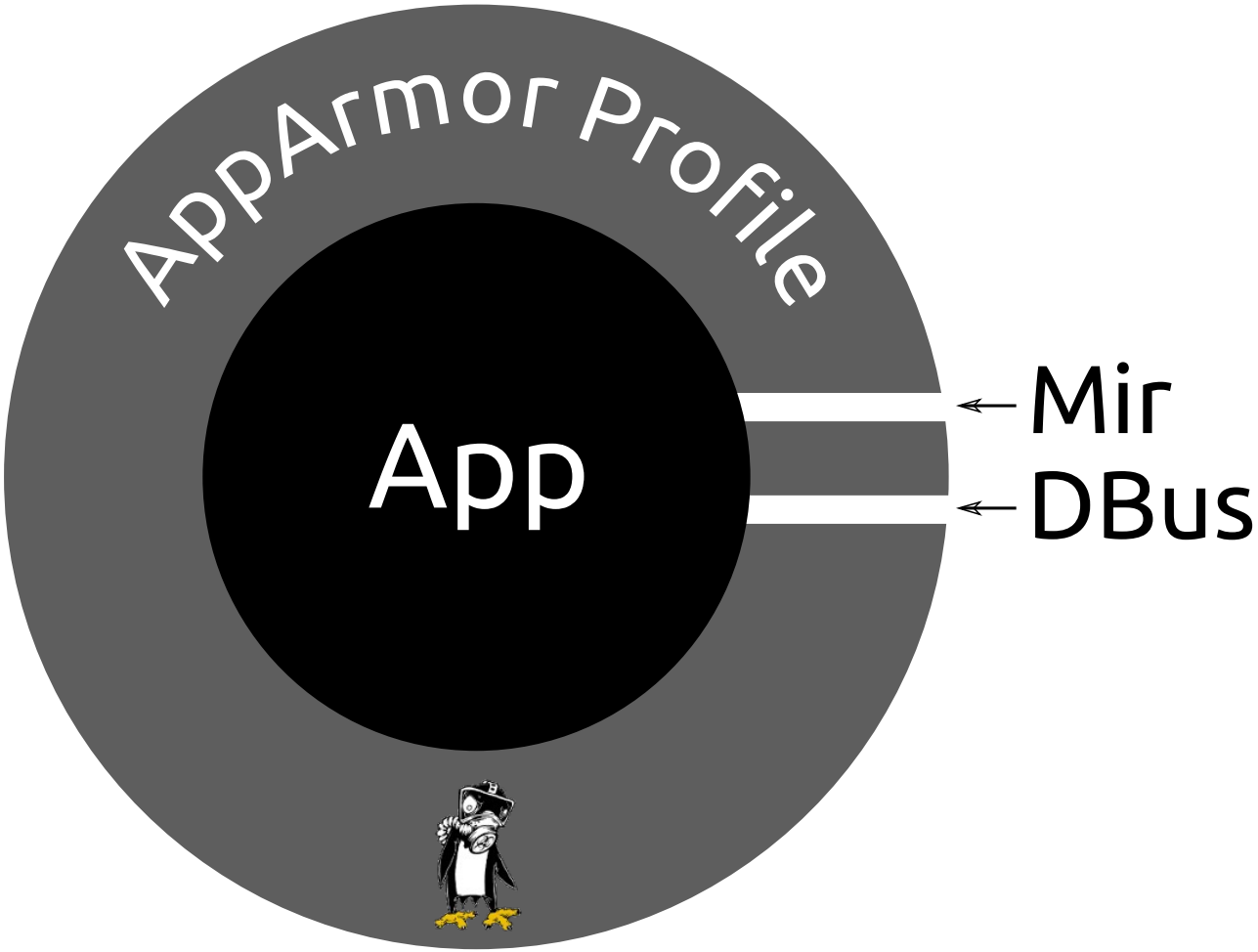
Stop using processing when not asked

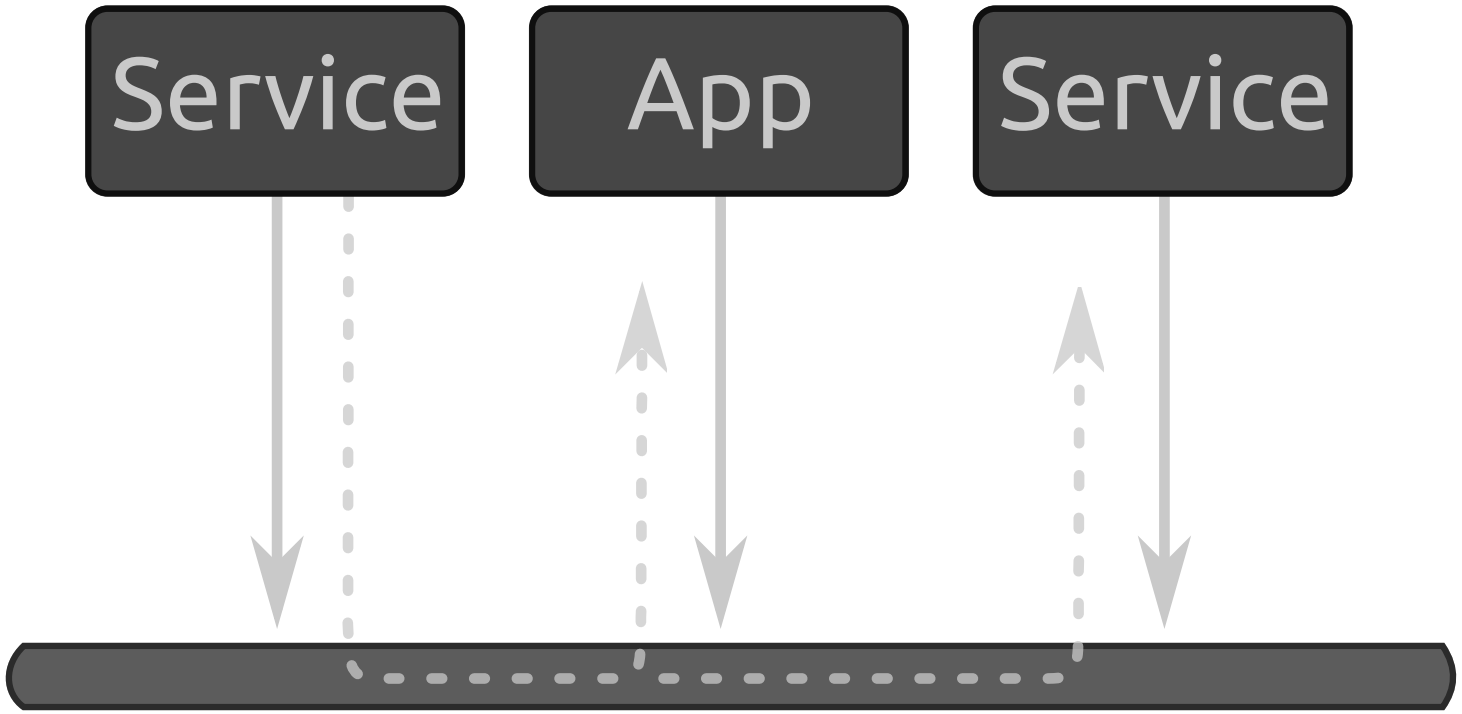
Negative:

SIGSTOP apps

SIGKILL apps on OOM killer

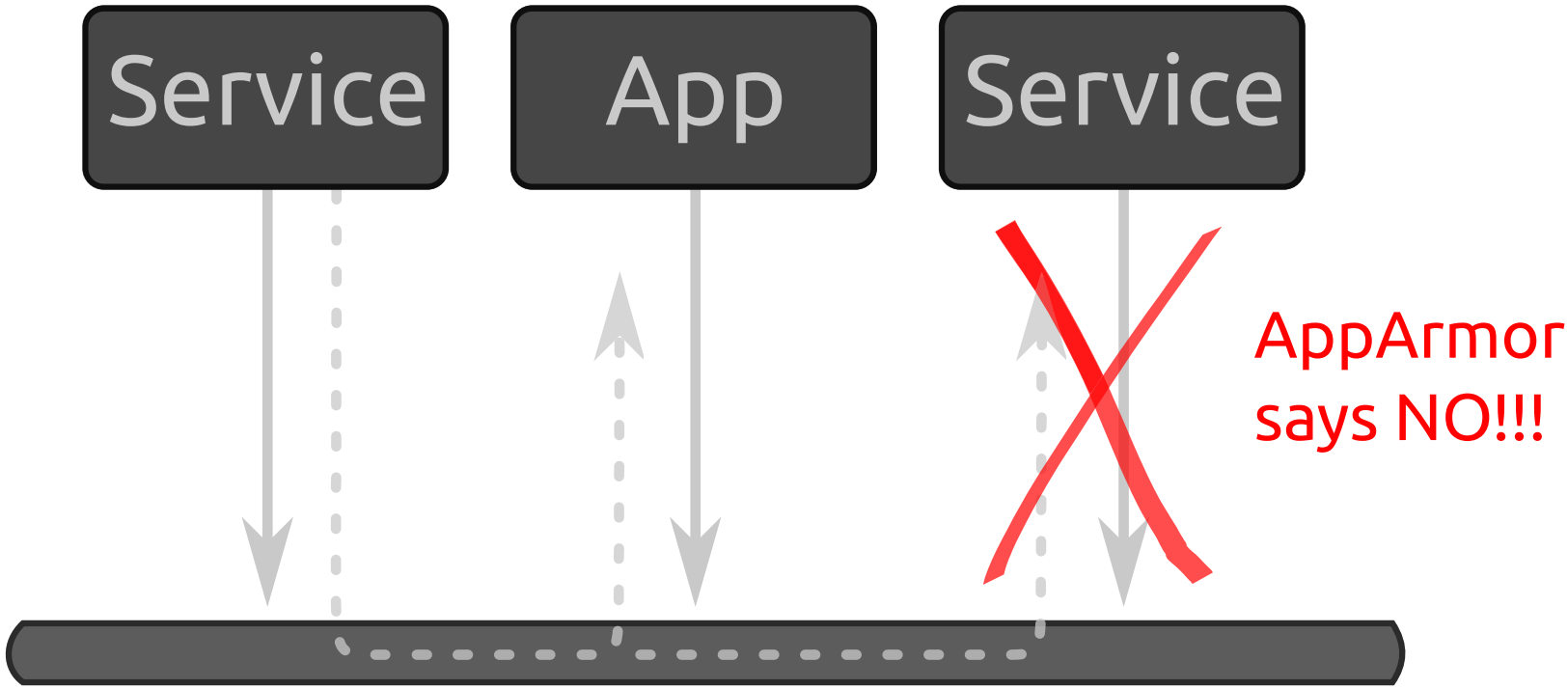

Likely to be killed
Stopped App
Untrusted Helpers
Active Application
Unity

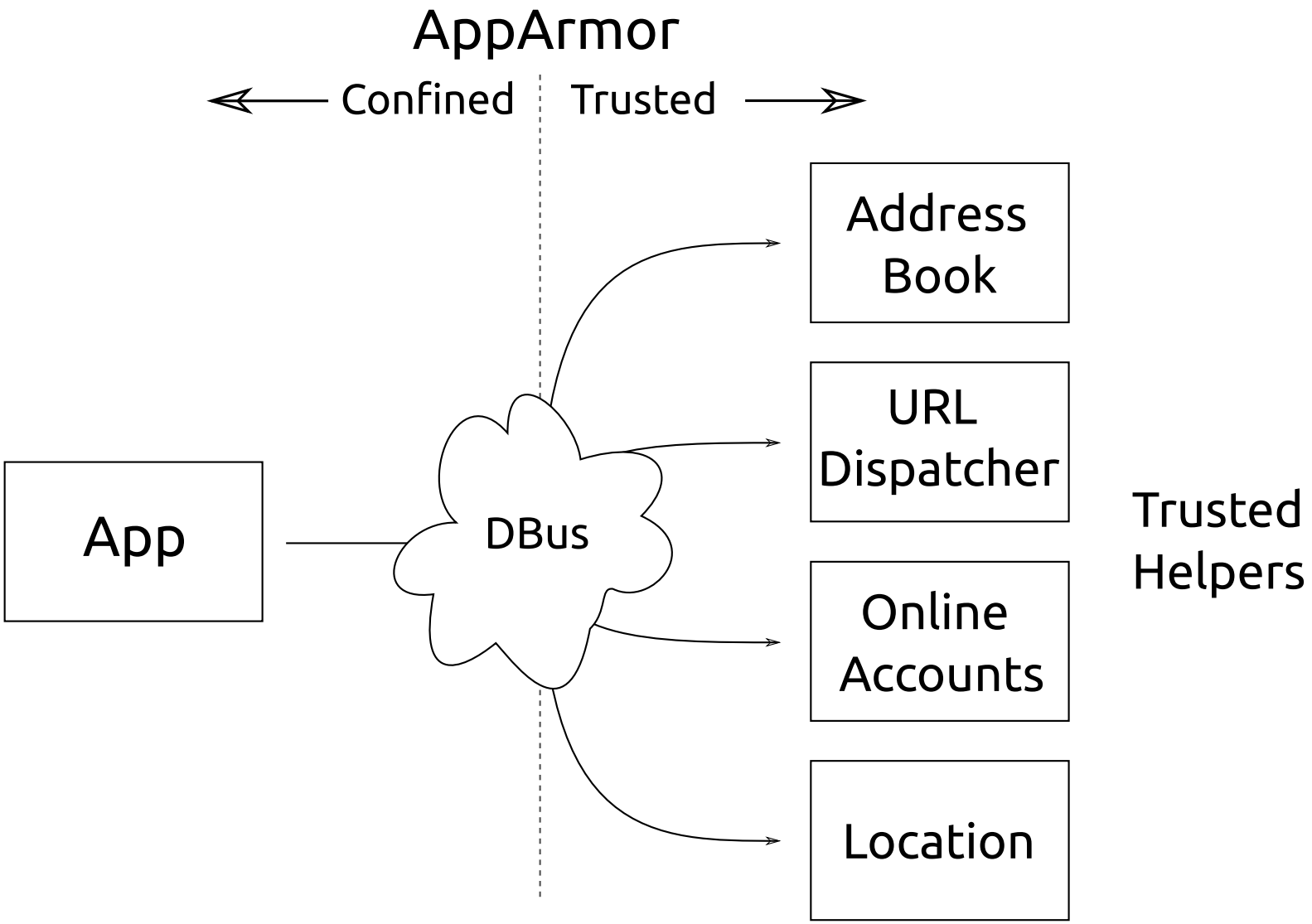

AppArmor Profile
App
Mir
DBus

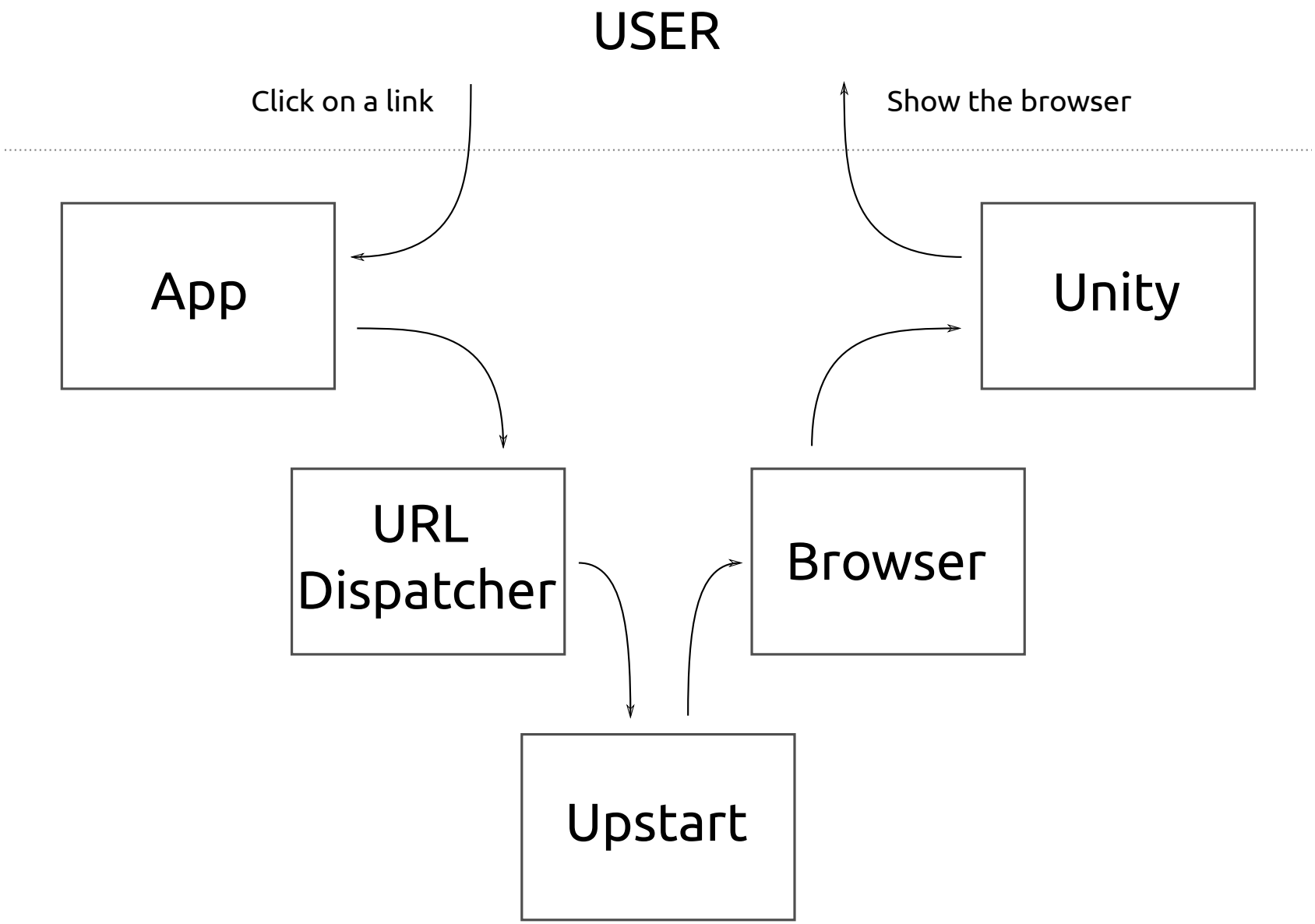

Service
App
Service
DBus

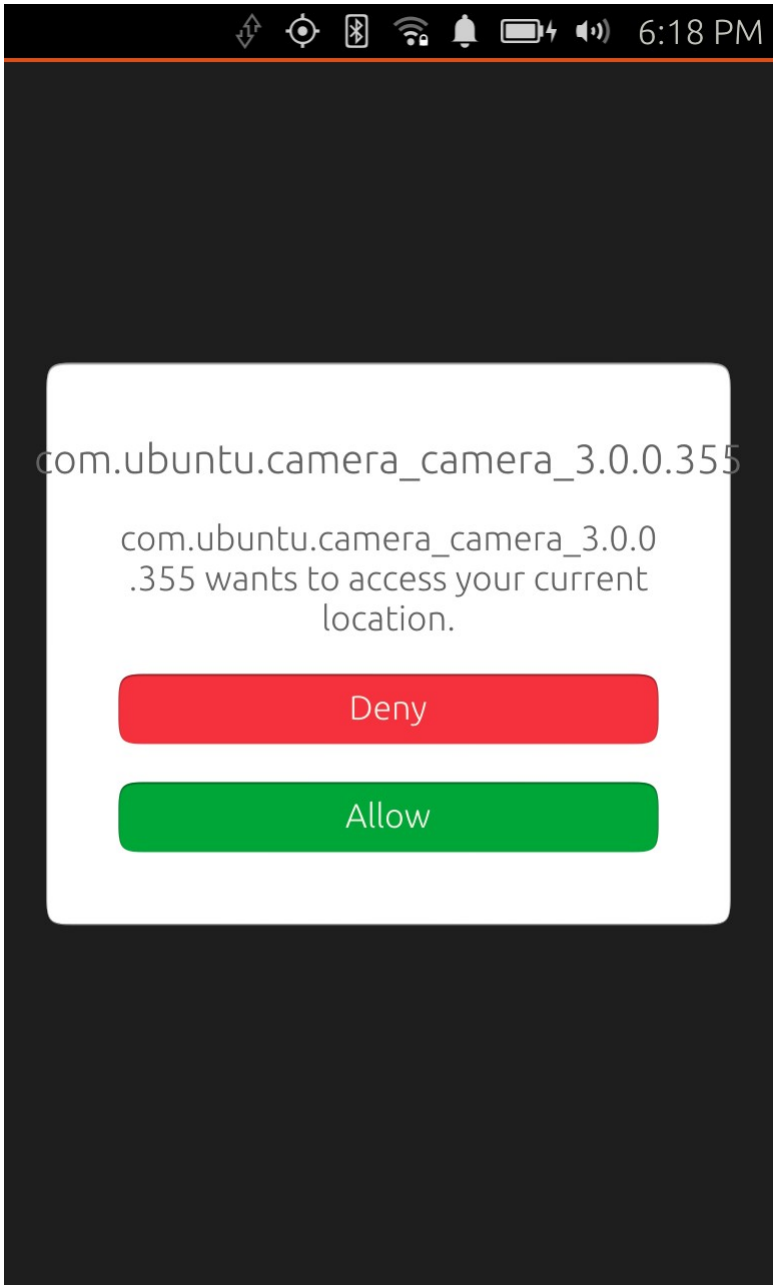
DBus Message

Header	
Type	Signal or Method
Destination	`:0.54` or “`com.canonical.Unity`”
Path	`/com/canonical/Unity/Dash`
Interface	`com.canonical.unity.dash`
Method	`ShowAttention`
Payload	[“foo”, “bar”]


Service
App
Service
AppArmor
says NO!!!


AppArmor
Confined
Trusted
Address Book
URL Dispatcher
App
DBus
Online Accounts
Location
Trusted Helpers


USER
Click on a link
Show the browser
App
Unity
URL
Dispatcher
Browser
Upstart



Request permission at time of use

Review (1/2)

Ubuntu Applications are[1]:

- ELF Binaries
- Link to C libs
- Draw on an EGL Buffer

[1] This is really only from a confinement/lifecycle perspective, we have a really nice QML SDK that makes application author's lives **much** easier, you should use it if you can.

Review (2/2)

Ubuntu Applications are:

- **Confined.** By default the applications are restricted from using a lot of functionality that might be expected from a traditional Linux user session.
- **Managed.** The application lifecycle works to keep the user in control of what is draining the battery and using resources.
- **Have Friends.** Trusted helpers provide ways to implement the functionality you need and work with confinement.

Additional Info

http://www.ubuntu.com/phone

https://developer.ubuntu.com

https://wiki.ubuntu.com/Security/AppArmor

https://wiki.ubuntu.com/Mir