

# SANDBOXED APPLICATIONS FOR GNOME

Allan Day

# Credits

William Jon McCann

Jakub Steiner

Lennart Poettering

Kay Sievers

Colin Walters

Alex Larsson



# Why sandboxing matters

Security and privacy

Application developer experience

Application distribution

OS definition

OS user experience

# Design principles

Avoid contracts

It doesn't have to look like security

Privacy not security

Real-time feedback

Audit and revocation

Temporary / one-time access

# Key design elements

Sharing

Content selection

System authorisation

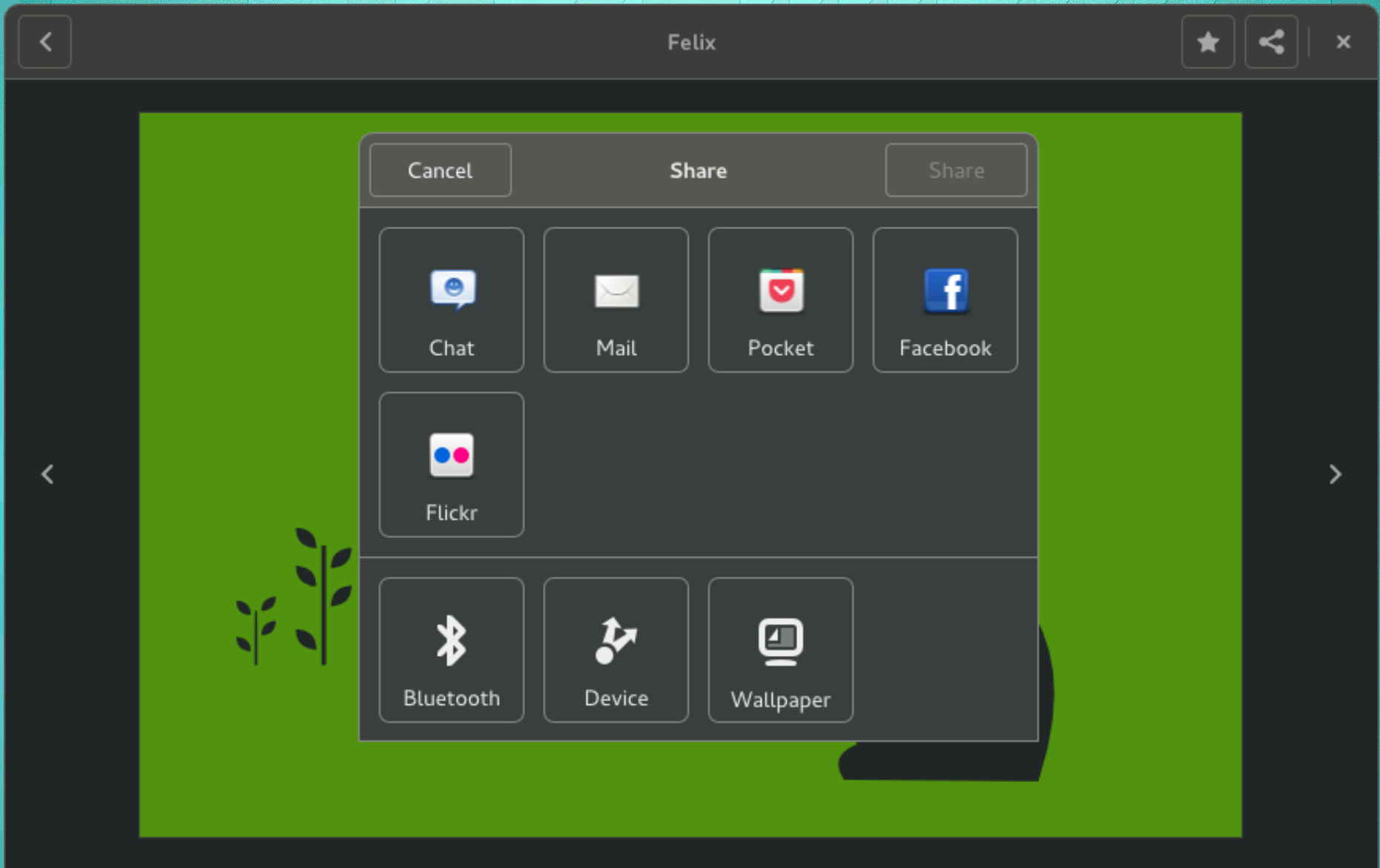
Real-time feedback

Audit and revocation

Sharing







# Content Selection



Cancel

### Select Items

Recent



Select



Friday Show Over Two Lines



order.pdf

Account	Type	DATE	AMOUNT
Account	Exp	02/14	100.00
Account	Exp	02/14	200.00
Account	Exp	02/14	300.00
Account	Exp	02/14	400.00
Account	Exp	02/14	500.00
Account	Exp	02/14	600.00
Account	Exp	02/14	700.00
Account	Exp	02/14	800.00
Account	Exp	02/14	900.00
Account	Exp	02/14	1000.00



expenses.xls



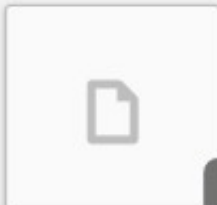
Project Plan



Morning Grass



Global Synergy Procurement



Applications

















← **Select Items** 🔍 Select  
Recent Files











- 🕒 Recent
- ★ Starred
- 🏠 Home
- 📁 Documents
- ⬇️ Downloads
- 🎵 Music
- 📷 Pictures
- 📺 Videos

<input type="checkbox"/>		throw the ball.avi	18:45
<input type="checkbox"/>		summer_mix.ogg	16:05
<input type="checkbox"/>		Master Plan.odt	12:30
<input type="checkbox"/>		morning_grass.jpg	9.45
<input type="checkbox"/>		expenses.xls	23 Sep
<input type="checkbox"/>		conference plan.odt	23 Sep
<input type="checkbox"/>		comedy hour.ogg	23 Sep
<input type="checkbox"/>		schedule.odt	23 Sep
<input type="checkbox"/>		shep.jpg	23 Sep
<input type="checkbox"/>		car hire.pdf	22 Sep



3 Selected Recent Select

- Recent
- Starred
- Home
- Documents**
- Downloads
- Music
- Pictures
- Videos

<input type="checkbox"/>	 throw the ball.avi	18:45
<input type="checkbox"/>	 summer_mix.ogg	16:05
<input checked="" type="checkbox"/>	 Master Plan.odt	12:30
<input type="checkbox"/>	 morning_grass.jpg	9.45
<input type="checkbox"/>	 expenses.xls	23 Sep
<input checked="" type="checkbox"/>	 conference plan.odt	23 Sep
<input type="checkbox"/>	 comedy hour.ogg	23 Sep
<input checked="" type="checkbox"/>	 schedule.odt	23 Sep
<input type="checkbox"/>	 shep.jpg	23 Sep
<input type="checkbox"/>	 car hire.pdf	22 Sep

# System authorisation

3G

Camera

Content (Documents, Music, Pictures, Videos, ...)

Data (Contacts, Calendar)

Location

Microphone





### Turn On Camera?

Firefox wants to use your camera and microphone.

Don't ask for this application again

Cancel

Turn On

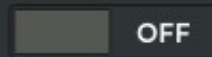




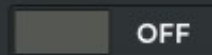
## Location Access

Firefox wants to know where you are. Turning on GPS and Wi-Fi will provide more accurate location information.

GPS



Wi-Fi



Search to manually set your location



Give Firefox location data in the future

Don't Allow

Allow





## Access Request

Angry Birds is requesting access to your content.

Contacts

Documents

Music

Videos

Don't ask again for Angry Birds

Don't Allow

Allow

**Real-time feedback**





Wi-Fi My Home Network ▶

Camera On ▼

Turn Off

Privacy Settings

Battery 2:10 Remaining (60%) ▶





Control Center panel with the following elements:

- Volume slider (Speaker icon)
- Brightness slider (Sun icon)
- Wi-Fi: My Home Network (Wi-Fi icon)
- Location: On (Location icon)
- Turn Off (Text)
- Privacy Settings (Text)
- Battery: 2:10 Remaining (60%) (Battery icon)
- Bottom navigation: Settings (Wrench icon), Lock (Lock icon), Power (Power icon)



# Audit and revocation



## Privacy



Privacy controls allow you to decide which applications can access your data and hardware.

3G	Yesterday
Calendar	In use
Camera	Never used
Contacts	In use
Documents	In use
Location	10 May
Microphone	Never used



## Location



Location services allow applications to determine your geographical position.

Location Services

ON

GPS and Wi-Fi increase the accuracy of location positioning.

Wi-Fi

ON

GPS

ON

### Applications



Photos

In use

ON



Documents

Yesterday

ON



Music

7 May

OFF



Videos

10 May

OFF



## Contacts



Contacts access allows applications to view your contacts.

Contacts Access

ON

### Applications



Photos

In use

ON



Documents

Yesterday

ON



Music

7 May

OFF



Videos

10 May

OFF

**Thank you!**

[wiki.gnome.org/Design/Whiteboards/ApplicationSandboxing](http://wiki.gnome.org/Design/Whiteboards/ApplicationSandboxing)

