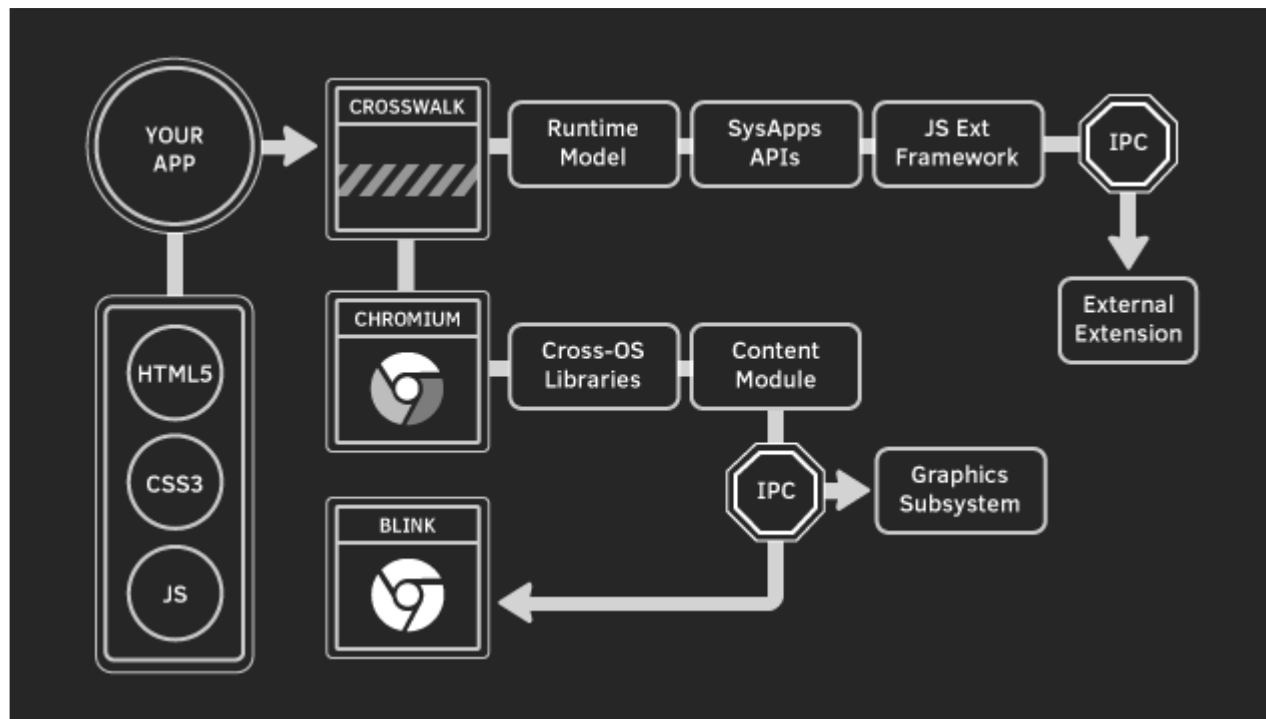


Crosswalk on Tizen

Tizen Security F2F

Vannes, France
Sept 2014
Terri Oda

Crosswalk Overview



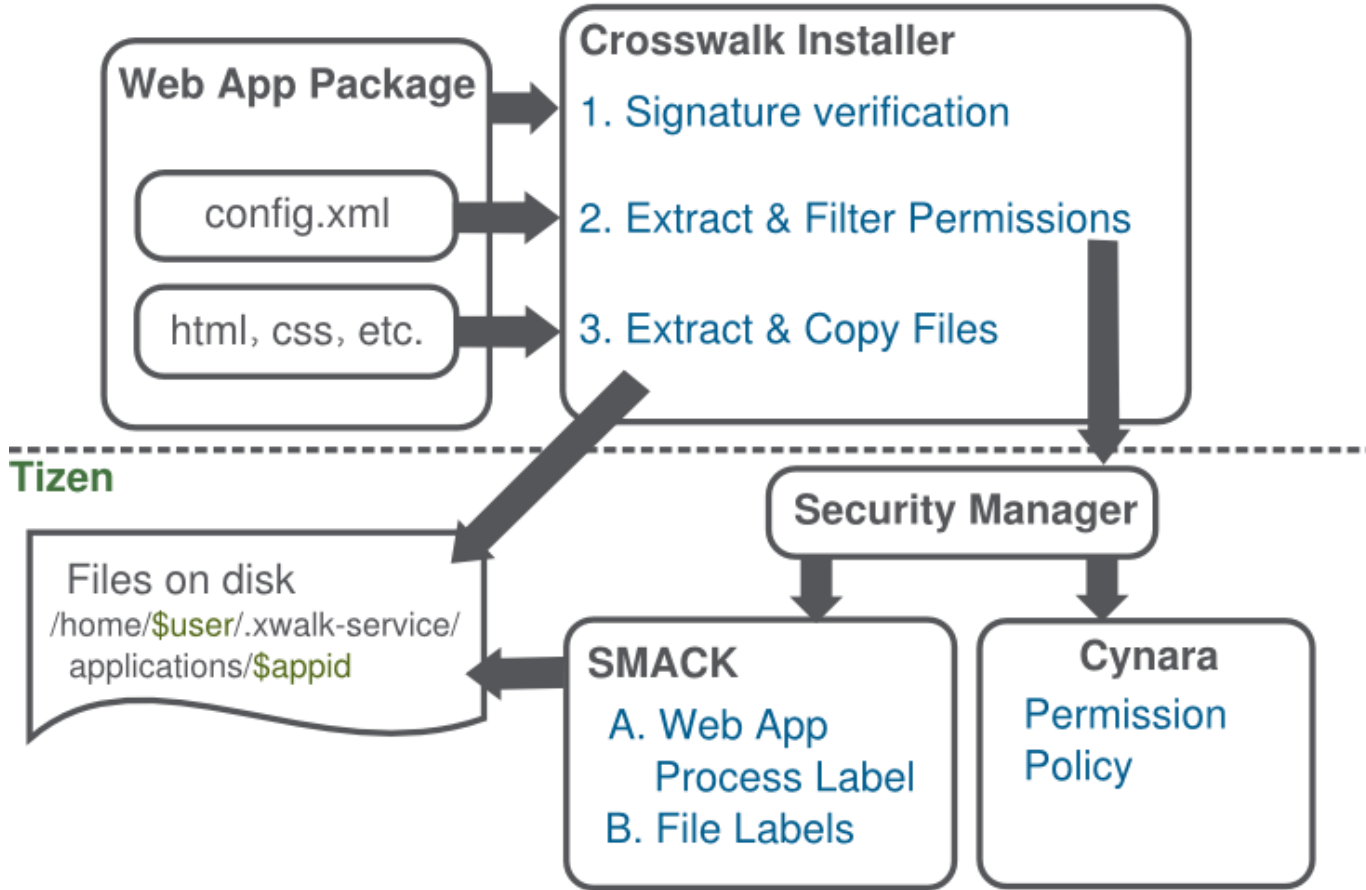
Application Installation

- Copies files to /home/\$**user**/.xwalk-service/applications/\$**appid**
- Sets Cynara rules using security-manager
- What about **extensions**?
 1. built-in extensions installed as part of platform in /usr/lib/tizen-extensions-crosswalk/
 2. 3rd party extensions – installed with application



Crosswalk Installer

Crosswalk

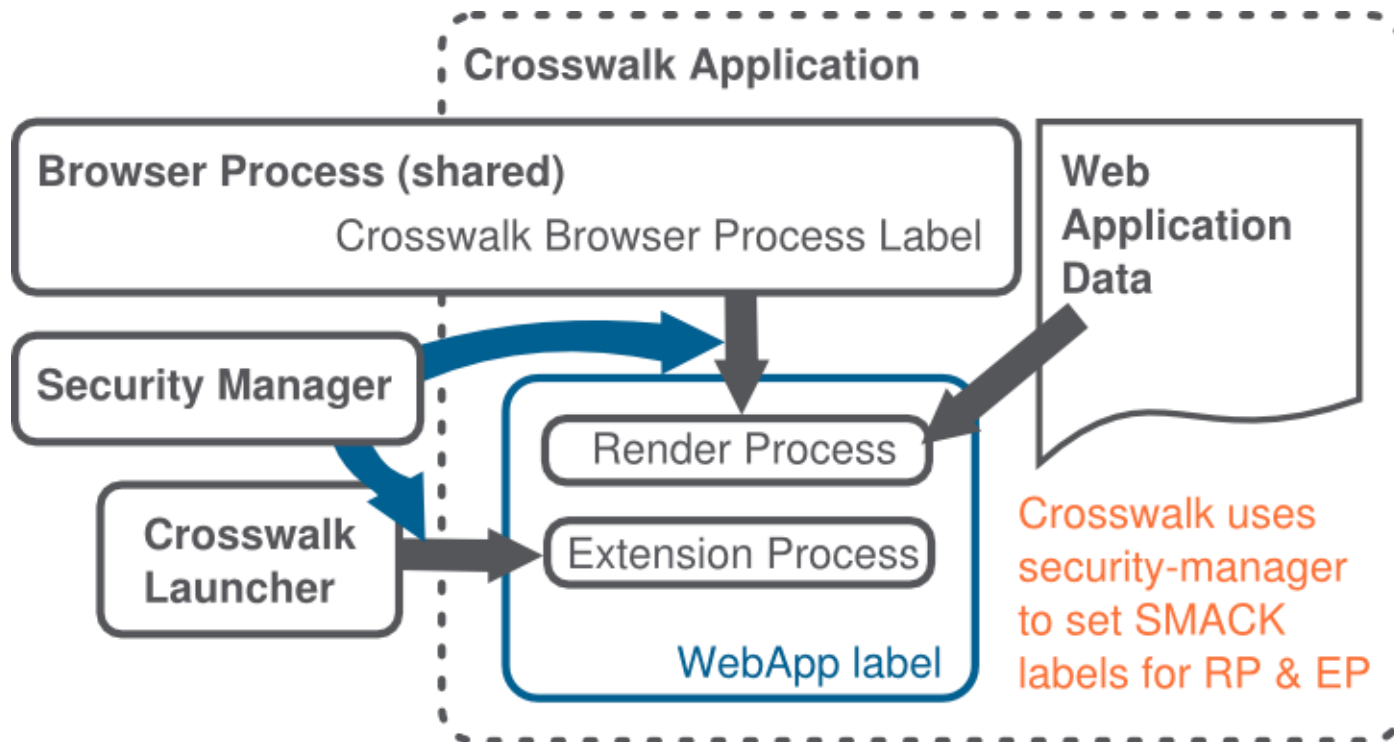


Application Launcher

- Launcher forks to create extension process
- Browser forks to create render process
- Each one sets SMACK labels for those processes using security-manager



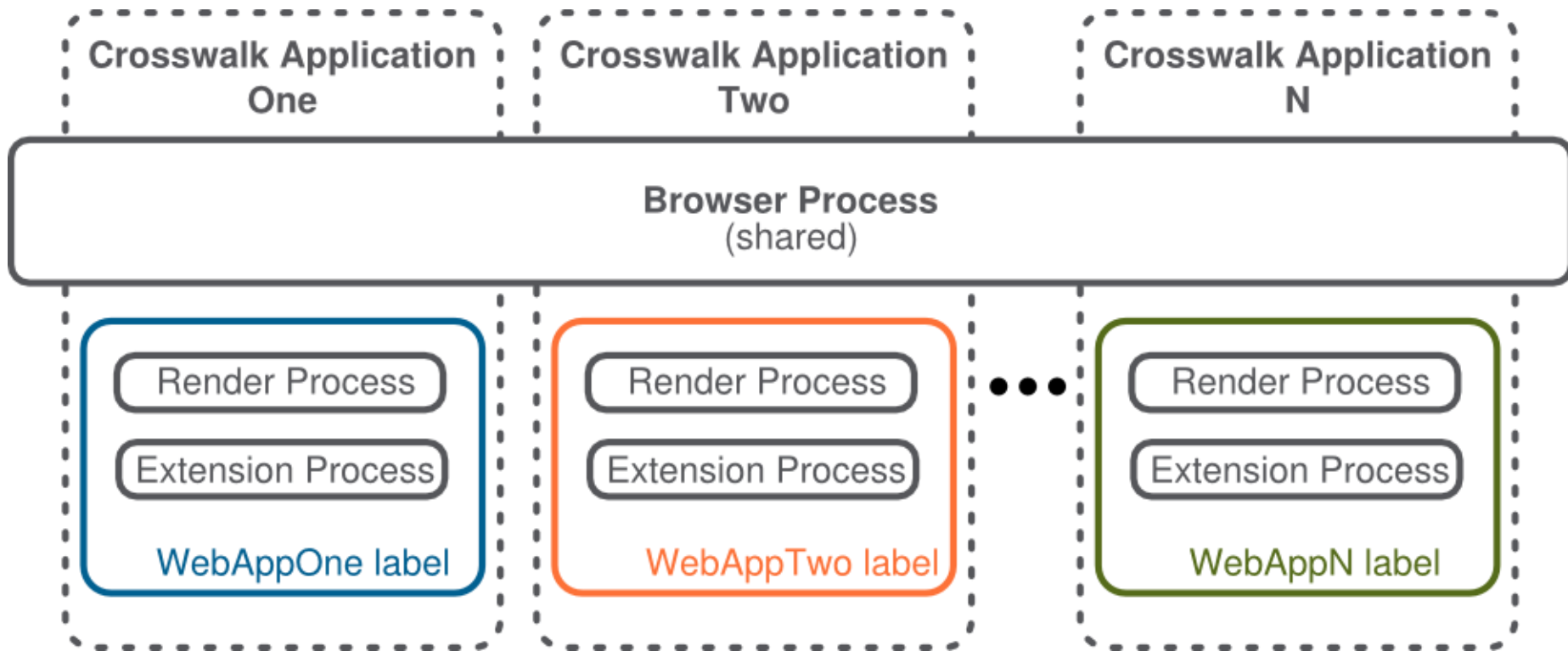
Crosswalk Launcher



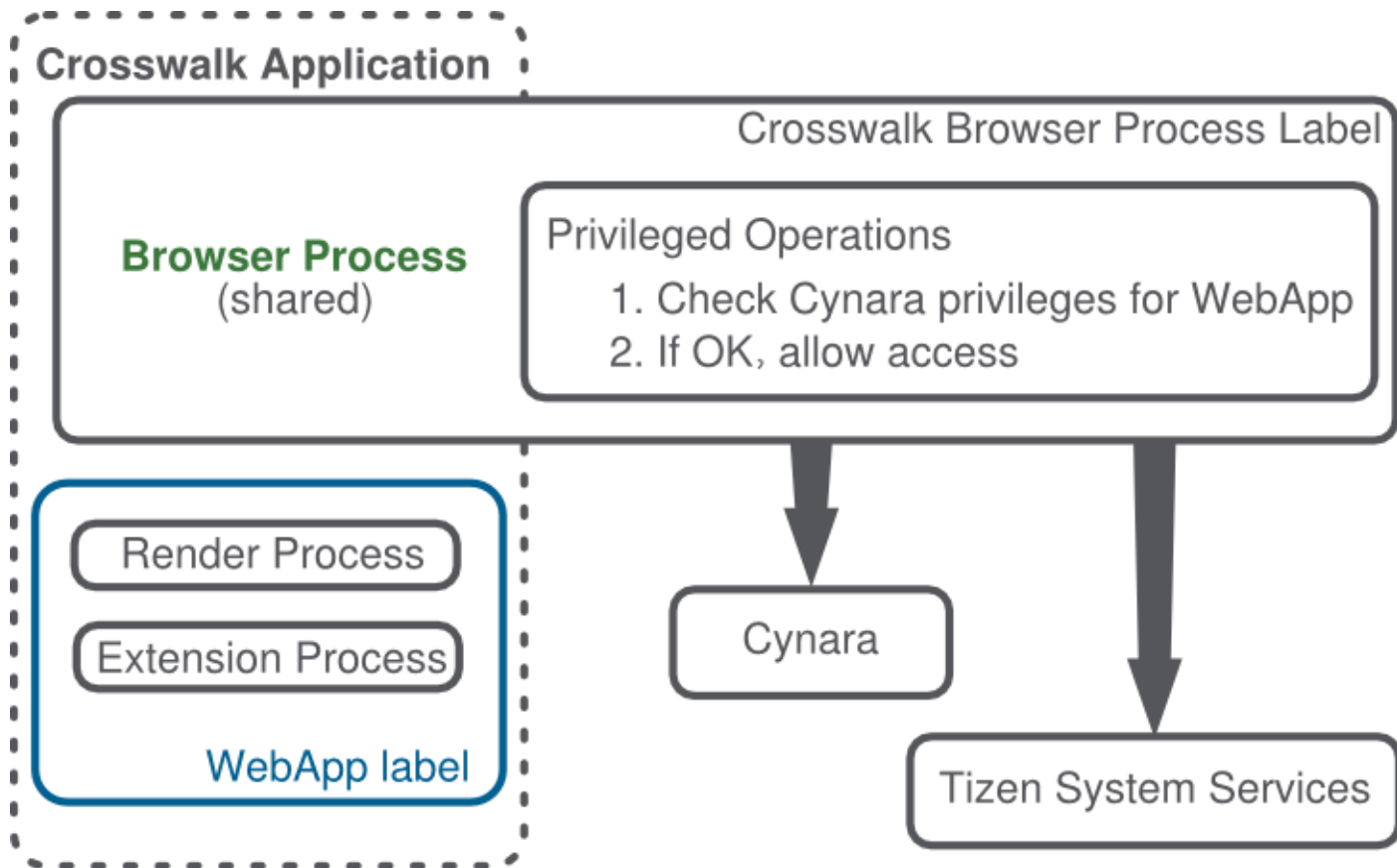
Crosswalk Runtime

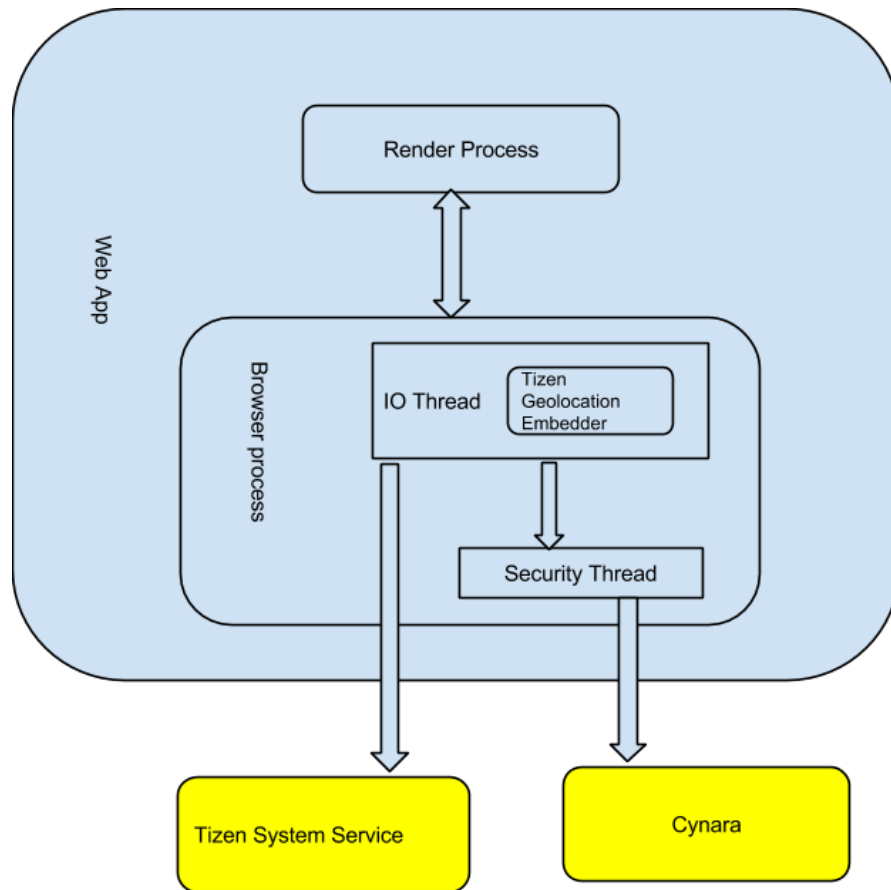
- Extension Process and Render Process run under WebApp-specific SMACK label
 - We have to treat this is code that is both untrusted and requiring our protection
 - Any permissions requested are handled by Tizen OS
- Browser Process is shared, runs under separate label
 - Aware of SMACK label for WebApp, uses that to query Cynara (directly) to check permissions
 - Browser Process actually only handles 5 privileges, rest are in extension process

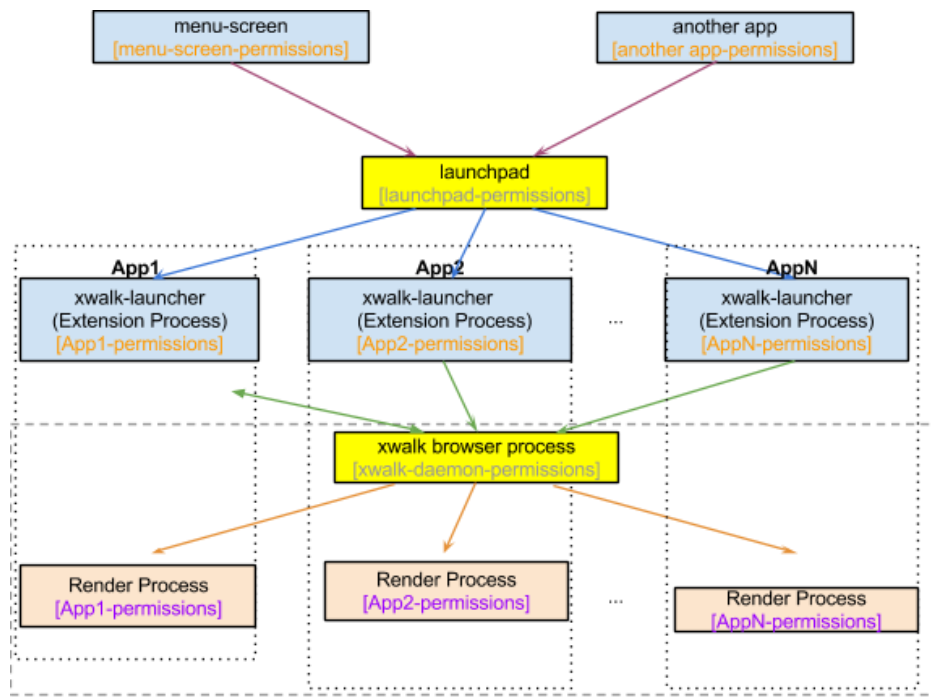




Crosswalk Runtime







Legend:

toplevel session child process	[permissions applied by session]
launchpad child process	[permissions applied by launchpad]
xwalk child process	[permissions applied by browser process]

The general process is as below:

1. user trying to launch an application by clicking the application icon in home screen or another application throwing an intent to launch web app, which result in a series of IPC message passing between multiple processes and eventually the launchpad_daemon is notified of this action.
2. The launchpad_daemon fork a child process xwalk-launcher and xwalk-launcher create a new xwalk extension process instance. xwalk-launcher set SMACK label for itself.
3. xwalk-launcher send an dbus message to running application manager (Browser process). Application manager launch web application and start a new render view(render process)/
4. Render process set itself SMACK label Render process adds itself to required supplementary groups. To be allowed to do that, it also needs CAP_SETGID capability.

Cynara/security-manager issues

- Some permissions require explicit user consent (e.g. download a page): will cynara/security-manager provide a way to check with the user? (pop-ups?)
- Security-manager: How will this dialog be configured?
- Dropping privilege with security-manager?
- What privileges will change in Tizen 2 -> Tizen 3?



Application Signatures

- Are we doing application signatures?
- Old web runtime only allowed privileges based on application signatures – will we do the same?
- Is there any differentiation based on signature for the application privileges?
- Must be able to check fingerprint of key against preloaded list of certificates
 - Currently there is no mapping
- How do we configure the privilege level for a certificate?



Content Security Policy (CSP)

- Not fully implemented (although Chromium/Blink supports already)
 - Plan is to read from manifest
 - W3C standard is still being defined
- Tizen has a default security policy (inherited from WRT)
 - Note that this is not true on other crosswalk platforms
- Crosswalk does not enforce CSP on extensions



Troika pictures

1. [janwillemssen](https://www.flickr.com/photos/8725928@N02/7061257609) vervoer Liebig- troika
<https://www.flickr.com/photos/8725928@N02/7061257609>
2. "Troika akron" by Лена - Own work. Licensed under Public domain via Wikimedia Commons
 - http://commons.wikimedia.org/wiki/File:Troika_akron.jpg#mediaviewer/File:Troika_akron.jpg
3. "PalekhTroikaWolves" by http://palekh.narod.ru/g/golikov/golii_04.jpg. Licensed under Public domain via Wikimedia Commons
 - <http://commons.wikimedia.org/wiki/File:PalekhTroikaWolves.jpg#mediaviewer/File:PalekhTroikaWolves.jpg>
4. http://bestspb.ru/imgs/russian/russian_troika1.jpg
5. http://www.horses.ru/horsemanship/main_troika.htm
6. <http://www.56thparallel.com/wp-content/uploads/2013/07/troika-race.jpg>

Q & A