Tizen 3.0 中的 Crosswalk 安全性

Xu Zhang(xu.u.zhang@intel.com)

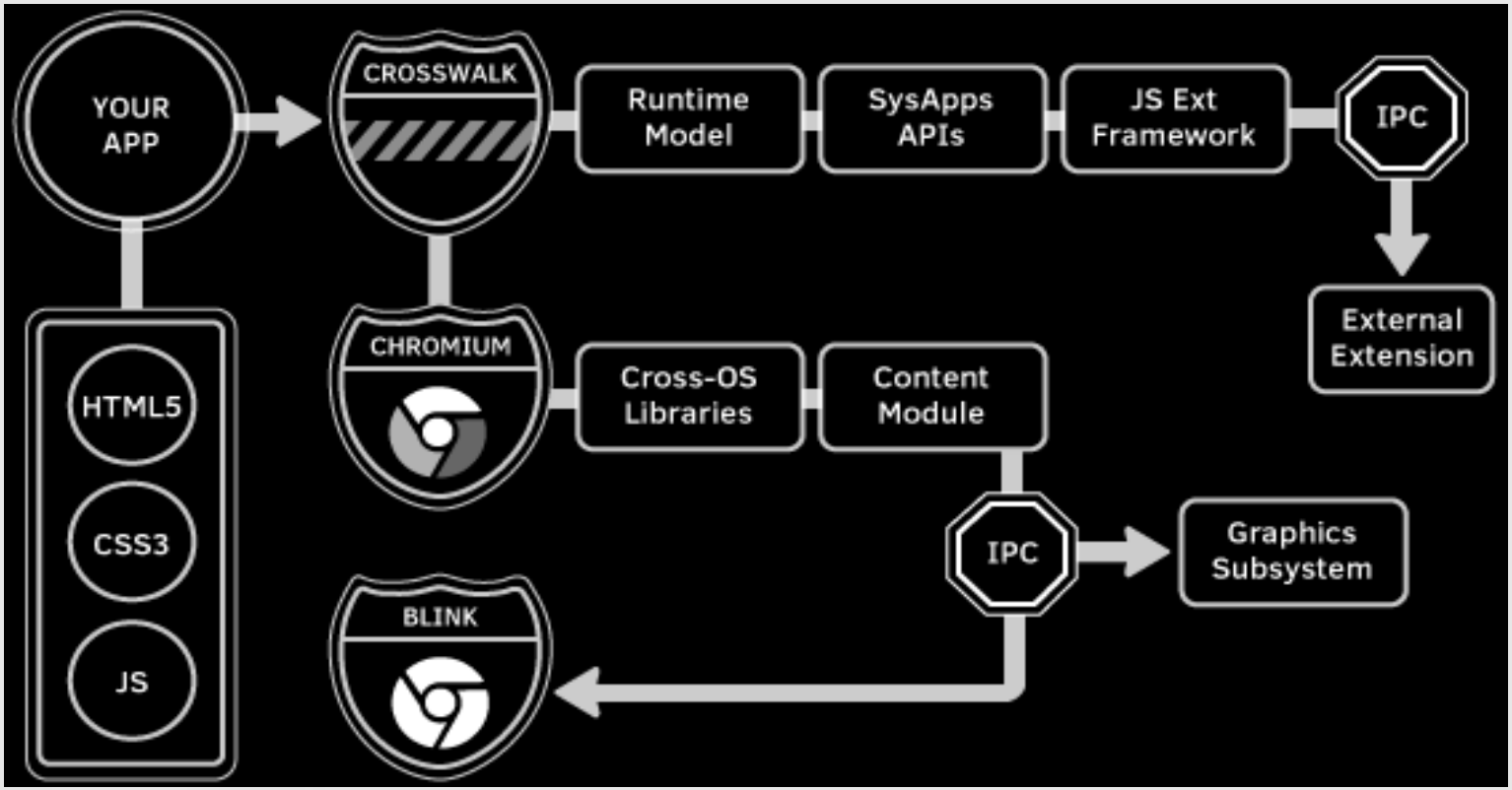
议程

- Tizen 3.0 安全性概述
- Crosswalk 概述
- Crosswalk 安全特性
- 结论
- 帮助完善 Crosswalk

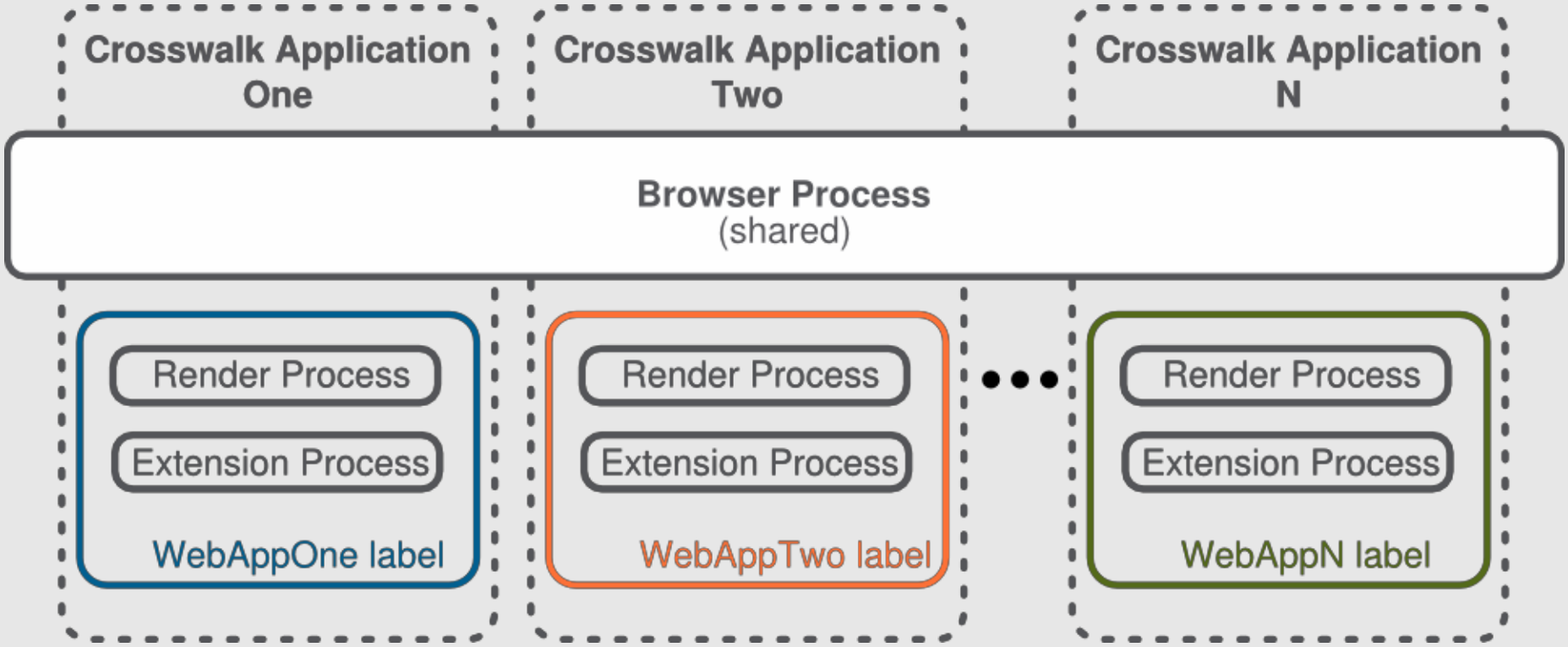
Tizen 3.0 安全性概述

- 目标：
  - 保护用户数据
  - 保护系统资源（包括网络）
  - 提供应用隔离
- **Tizen 3 提供重要的安全特性：**
  - 自主访问控制 (DAC)
  - 借助内核 LSM SMACK 的强制访问控制 (MAC)
  - Cynara 权限管理和检查服务
  - 安全管理器

Crosswalk 概述



Crosswalk 针对每用户共享处理模式



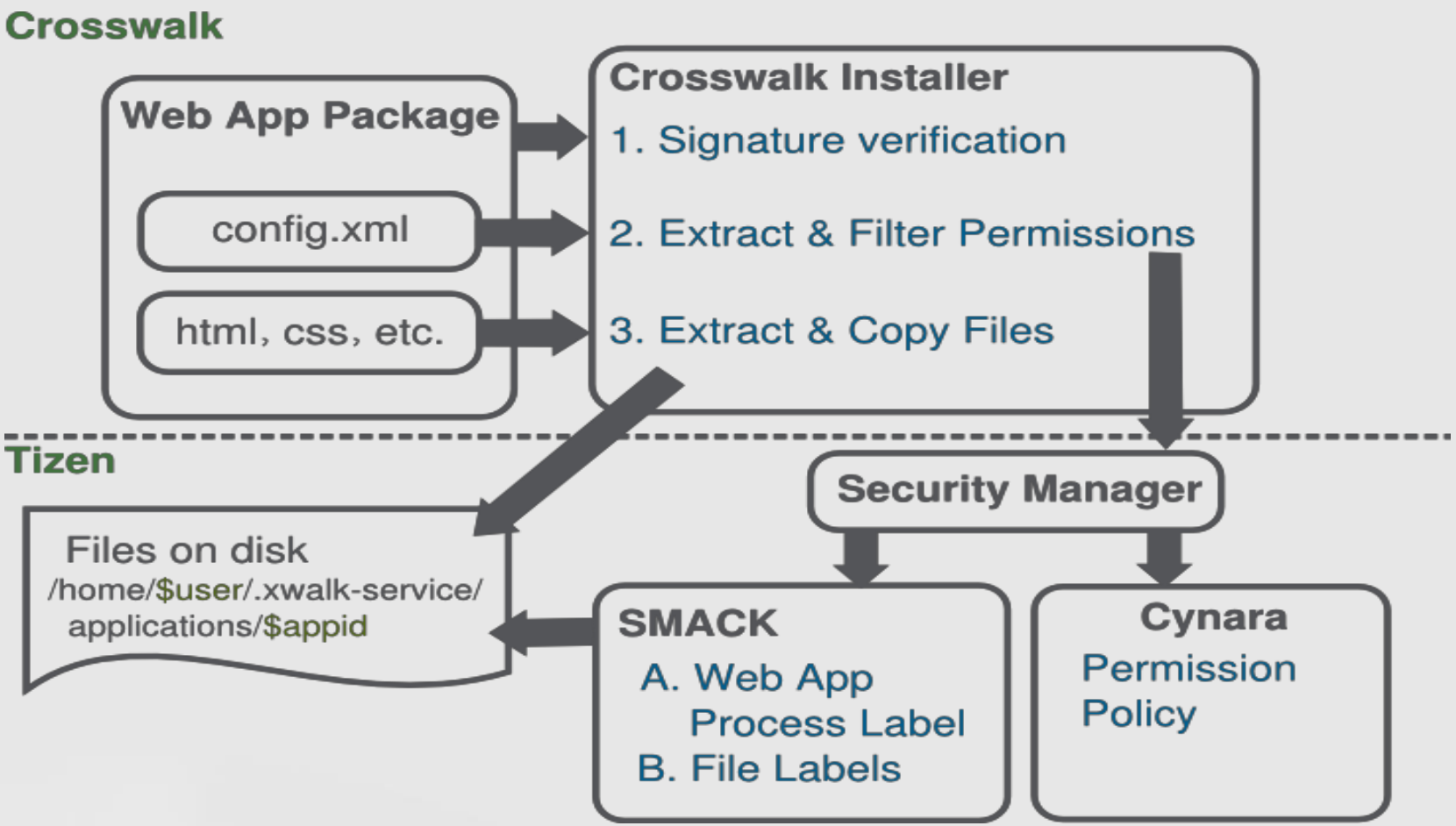
Crosswalk 安全特性

- 与 **Tizen 3.0** 安全性的关系
  - 在SMACK、Cynara 和安全管理器之上构建
- **API** 访问控制
- **web** 小部件应用签名
- **CSP**（内容安全策略）
- **WARP**（小部件访问请求策略）

API 访问控制

- 插入/更新权限策略
- 设置 **SMACK** 标签
- 运行时间检查

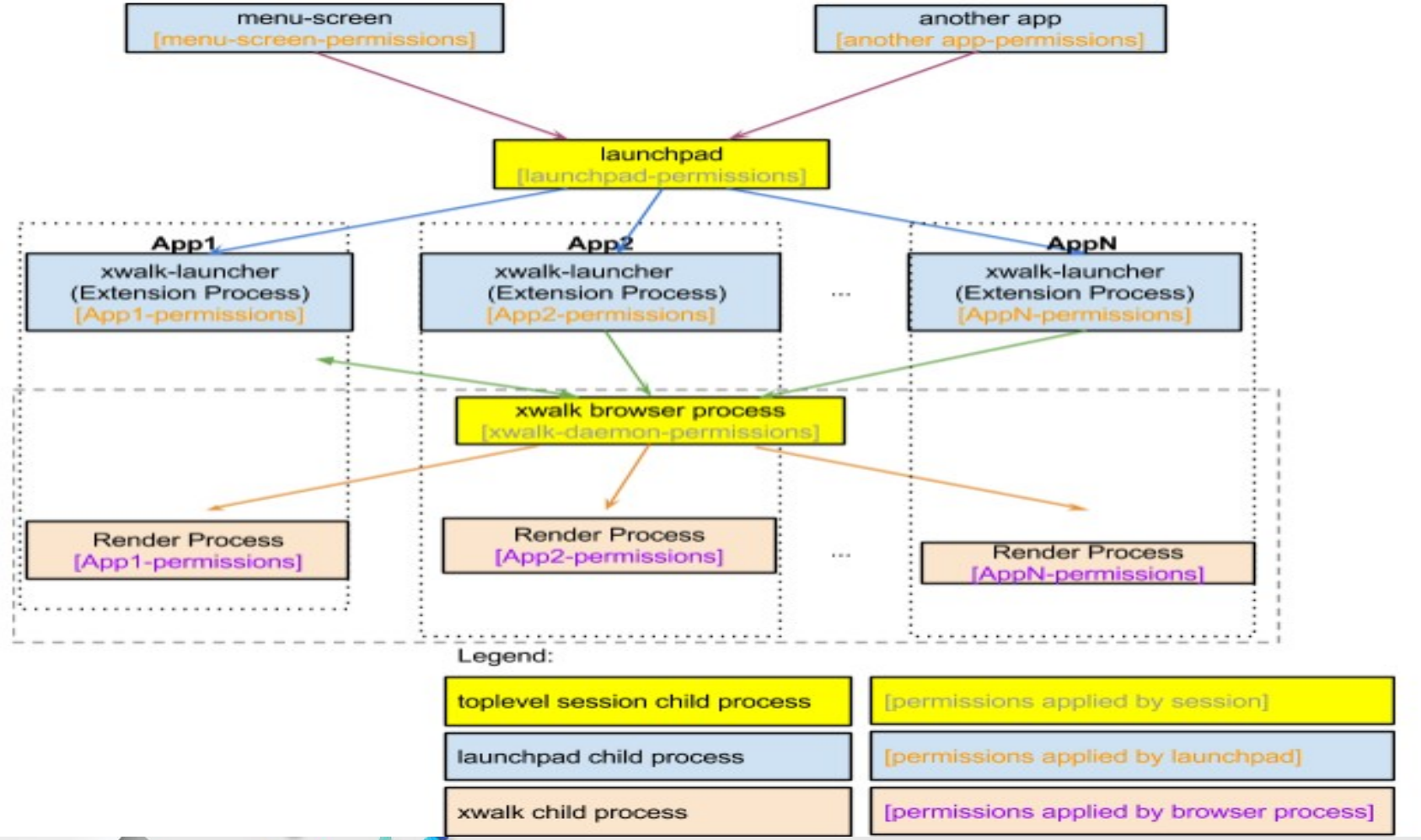
API 访问控制 - Crosswalk 安装程序



API 访问控制 - Crosswalk 安装程序 （续）

- 安装 **web** 应用的一般流程
  1. Crosswalk 安装程序解压 Crosswalk web 应用软件包
  2. Crosswalk 安装程序验证软件包的签名
  3. Crosswalk 从 config.xml 中提取权限列表
  4. 根据权限级别，Crosswalk 从权限列表中过滤出无效权限
  5. Crosswalk 安装程序调用安全管理器，为资源插入策略文件和权限

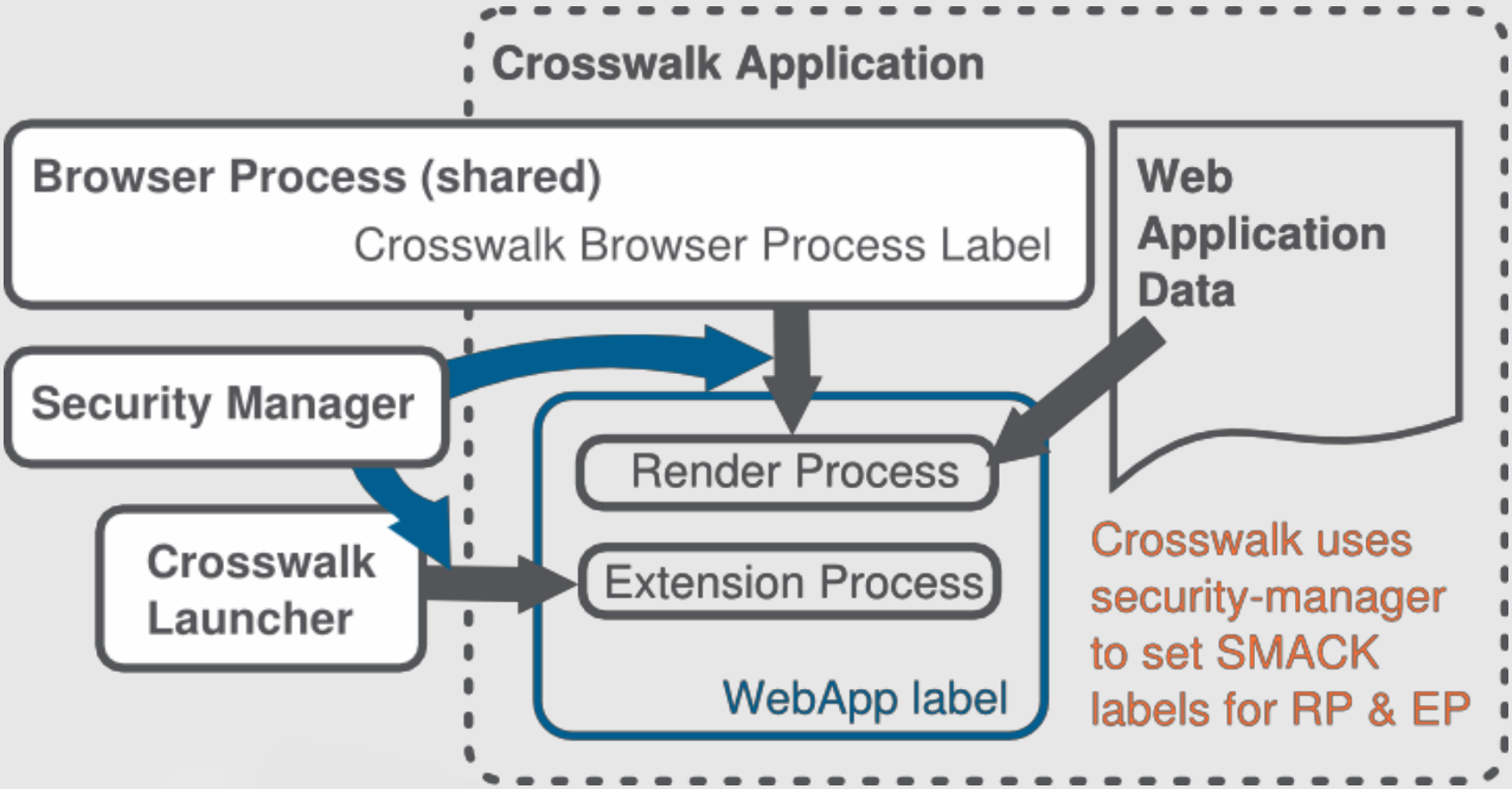
API 访问控制 – 启动器



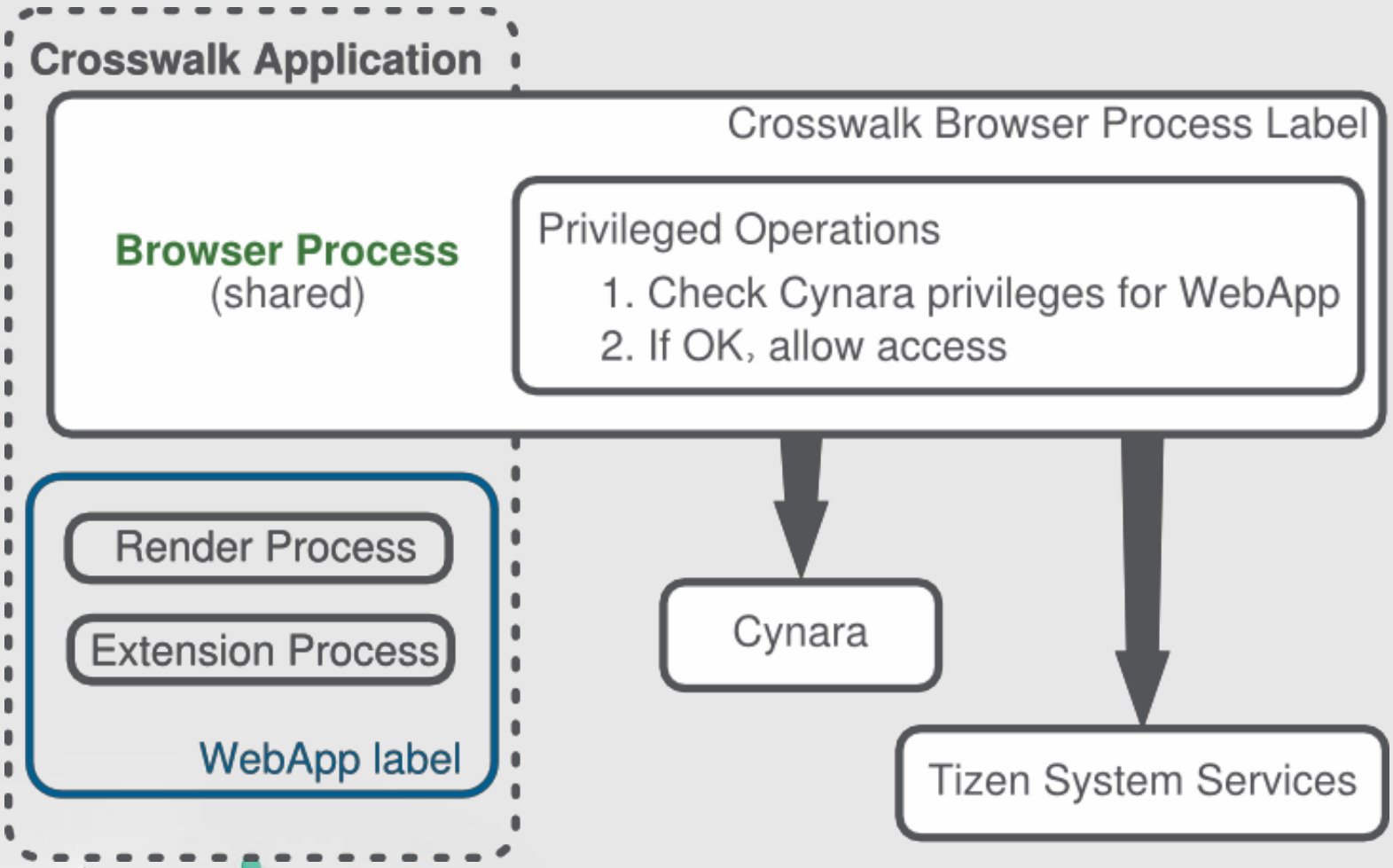
API 访问控制 – 启动器（续）

- 启动 web 应用的一般流程
  1. 用户点击主屏幕上的应用图标或想要启动 web 应用的另一个应用，尝试启动应用。
  2. launchpad_daemon 对 xwalk-launcher 子进程进行分叉处理（fork），xwalk- launcher 创建一个新的 xwalk 扩展进程实例
  3. xwalk-launcher 向运行的应用管理器发送一条 dbus 消息（浏览器进程）。应用管理器启动 web 应用，并启动一个新的渲染视图（渲染进程）

API 访问控制 – 设置 Smack 标签



API 访问控制 – 运行时检查



API 访问控制 – 运行时检查（续）

- **检查 API 访问的一般流程**
  1. 敏感的 W3C JS API 被调用时，渲染进程向运行时进程发送 IPC
  2. 运行时进程请求 Cynara 检查 API 权限
  3. Cynara 将 ALLOW/DENY 返回至运行时进程
  4. 如果操作被允许，运行时进程将访问 Tizen 系统服务

应用 签名

- **Tizen WGT** 应用必须有两个签名：
  - 作者签名
  - 发布者签名
- 基于对 **XML** 数字签名的 **W3C** 推荐
- **Crosswalk** 验证应用是否已使用证书进行了正确签名
- 决定 **web** 应用的权限级别
  - 平台
  - 合作伙伴
  - 公共
  - 不可信

内容安全策略 (CSP)

- 对于由 **web** 应用加载或执行的资源，**CSP** 会充当白名单机制
- 策略通过应用清单（如下）进行定义

```
{
…,
"content_security_policy":"[POLICY STRING GOES HERE]”
…
}
```

- **Crosswalks** 中的 **CSP** 支持基于 **Chromium** 和 **Blink** 实施
- **Crosswalk** 不会在扩展上强制实施 **CSP**

小部件访问请求 策略 (WARP)

- 在默认状态下，小部件的所有网络访问操作都会被拒绝
- 小部件必须在清单中声明其将访问哪些网络资源（如 XMLHttpRequest、iframe、img、脚本等）。

- 在默认状态下，小部件的所有网络访问操作都会被拒绝
- 小部件必须在清单中声明其将访问哪些网络资源（如 XMLHttpRequest、iframe、img、脚本等）。

```
<widget xmlns="http://www.w3.org/ns/widgets">
<widget xmlns
                ="http://www.w3.org/ns/widgets
<access origin=https://example.net                ">
<access origin=https://example.net
                                                  subdomains="false"/> />

</widget>
```

结论

- 开发人员：
  - 您需要在清单中声明所需权限
  - 请声明您真正需要的最小权限集
  - 注意在应用中进行适当的错误处理

帮助完善 Crosswalk

- 项目网址：
  - https://crosswalk-project.org
- 邮件组：
  - crosswalk-help
  - crosswalk-dev
- **IRC:**
  - #crosswalk at irc://freenode.net
- 漏洞跟踪：
  - https://crosswalkproject.org/jira/

鸣谢

- 感谢 Terri Oda、Casey Schaufler、Xinchao He 和 Peter Wang 作出的贡献

问题？

TIZEN™

开发者峰会

2014

上海

fil!:mlmiil.9fil!:mlmiil.9fil!:ml

TIZENTF:At ll$ (..t fi)