WebRuntime in Tizen

Janusz Majnert
Samsung R&D Institute Poland

Agenda

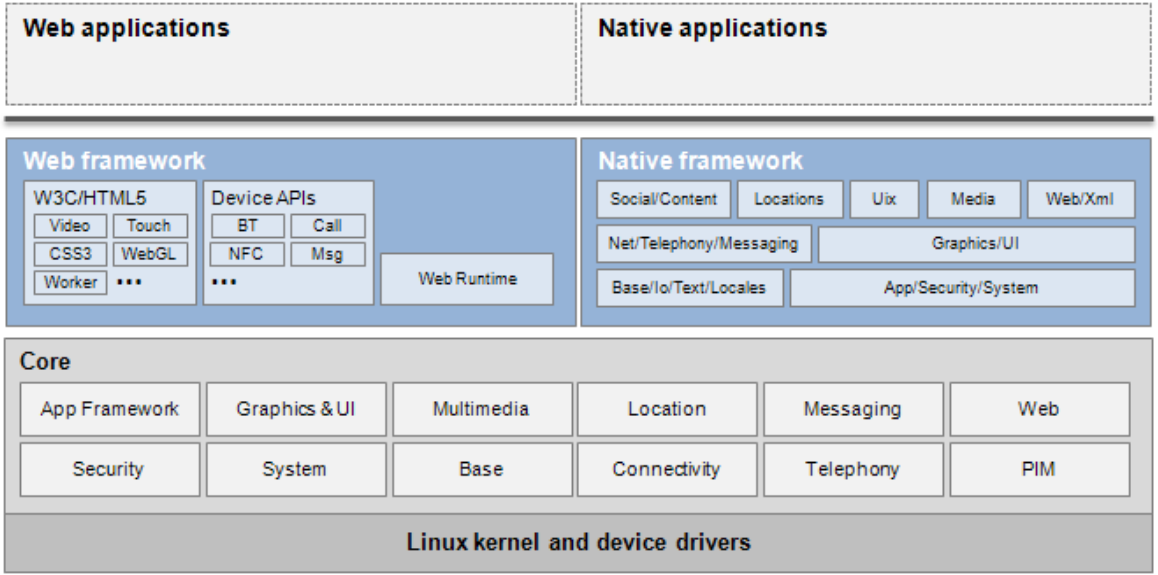
- Introduction to WebRuntime
- History outline
- APIs
- Web Browser Security
- Closing Security Holes in Browsers
- Additional Security Mechanisms in Tizen WebRuntime
- Standardization
- Future
- Tizen WebRuntime Future

Introduction to WebRuntime

Introduction to WebRuntime

What it is:

- Virtual machine
- Application manager



Web Application Execution Platform

Introduction to WebRuntime

Why HTML and Javascript:

- **Ready**
- **Well known**
- **Popular**
- **Easy to experiment with**
- **Open, standardized**
- **Cross-platform**
- **Many open source runtime engines available !**

Introduction to WebRuntime

Web Application Manifest

- **A way for the author to express application's preferences:**
  - name, description, author's name, version, icon, locale information
  - screen size, fullscreen
  - provided services (for example Web Activities)
- **A way for the author to express application's requirements:**
  - required features, permissions

Manifest enables web applications to be installed on a device

Introduction to WebRuntime

	Packaged application	Hosted application
Package contents	All necessary resources (HTML, JS, CSS, media files) and the application manifest	Application manifest
Access to network	Yes	Yes
Offline use	Yes	Yes, with the use of App Cache
Code review by app store	All source code can be audited for security. Code will not change after installation.	Review possible, but code may be changed on the hosting servers
Access to sensitive APIs	It's possible to have full access to sensitive API's, if application is trusted	Application cannot be fully trusted, so access to some API's may be restricted
Delivery mechanisms	App Stores, Side-loading	App Stores, Side-loading, Installation directly from author's website

Introduction to WebRuntime

Commercial implementations

- Tizen
- Firefox OS
- Chrome OS
- HP WebOS (now LG)

History outline

History outline

- **Web-based execution environments are not a new idea**
  - Earliest attempt: Google Gears in 2007
  - Year 2009 witnesses plethora of solutions: Opera Widgets, Palm WebOS, PhoneGap
  - More mature solutions, with backing from large telecoms: BONDI, JIL, WAC
- **Tizen WebRuntime builds on top of the WAC2.0 specification:**
  - Similar runtime and security model
  - A new set of APIs
  - New security mechanisms

APIs

APIs

Tizen WebRuntime exposes a set of powerful APIs

- **Generic:**
  - Filesystem, Camera, Bluetooth, Settings, SystemInfo, Power, Time
- **Mobile-oriented:**
  - Messaging, Telephony, Call History, Contacts, Calendar, NFC, Network Bearer Selection, Secure Element

Full list available in Tizen developer guide

Access to APIs is guarded by security policies to prevent abuse

Web Browser Security

SAMSUNG

Web Browser Security

Same Origin Policy

- **Main security boundary for web applications**
- **Documents and scripts from different origins are separated**
  - No access to each other's DOMs
  - Can only XHR to own origin
- **"Policy" – not a strict rule:**
  - No single definition, every browser has it's own version
  - Notable exceptions: <img>, <script> -> XSRF, ambient authority

Web Browser Security

Javascript

- **Great language! It makes Gmail possible!**
- **It also makes this possible:**
  - eval(), setTimeout(), setInterval(), Function()
  - window.location="evil.com”
  - XSS
  - stealing/leaking private data

Closing Security Holes in Browsers

Closing Security Holes in Browsers

- **Browser security is based on plugging the largest hole**
- **Various per-use-case solutions**
  - Difficult to manage
  - Easy to break with new features
- **Security prompts for accessing sensitive features, like camera**
  - Pushing the responsibility on end-users
- **Light in the tunnel – first systematic security mechanisms**
  - CSP, CORS
  - Changes in upcoming versions of ECMA Script

Additional Security Mechanisms in Tizen WebRuntime

SAMSUNG

Additional Security Mechanisms in Tizen WebRuntime

- **Digital Signatures of applications**
  - Package integrity and authenticity guaranteed by distributor (app store)
- **BONDI security policy framework**
  - Control of which applications can access which sensitive APIs
- **Trust levels**
  - The more trusted an application is the more it can do
- **Widget Access Request Policy**
  - Controls what origins an application can connect to

Standardization

Standardization

- **W3C Device APIs Working Group**
  - Slow
- **W3C Web Applications Working Group**
  - Several high quality specification used by Tizen WebRuntime
  - Pushed ahead by Opera
- **JIL, BONDI, WAC**
  - Telecom driven, worldwide collaboration
  - Born out of frustration with slow W3C process
  - Ultimately failed – no backing from big names of web

Standardization

- **W3C System Applications Working Group**
  - A new runtime model
  - New, better mobile-oriented APIs
- **W3C Web Applications Working Group**
  - New APIs for web browsers
  - Web Application manifest
- **W3C Web Application Security Working Group**
  - Security mechanisms

Future

Future

- **Observable trend to move towards web-based environments**
  - Portability, easier integration with ”the cloud”
  - Faster development cycle
- **Web applications on par with native apps**
  - Capabilities
  - Performance
- **Portability between various devices, form factors, OSes**

Future

- **Migration of certain mechanisms and APIs to regular Web**
  - Some APIs, if done correctly may be made available in regular browsers
  - Application manifest
- **Migration of browsers in the direction of WebRuntimes**
  - Web is no longer a repository of documents
  - Web is a set of web applications
  - Time to switch from a document viewer model to an execution platform

Tizen WebRuntime Future

SAMSUNG

Tizen WebRuntime Future

- **Support for upcoming W3C System Applications standards**
  - New runtime model
  - New APIs
- **Possible compatibility with other runtime vendors**
  - Application portability
- **Performance and capabilities comparable to native code**

SmartDevCon²

12-14th September 2013 - Katowice, Poland