SONY
make.believe

Trusted hosted web apps for Firefox OS

Claes Nilsson
SoMC Technology Research - Advanced Application Labs

Background

- There are two main types of web applications:
  - **Packaged web applications**: Manifest and application content are installed on device.
  - **Hosted web applications**: Application content is retrived at runtime from network servers. A manifest may be installed on the device.

- *SoMC considers the advantages of hosted web applications (see next slide) and is evaluating a security model that allows hosted web applications access to sensitive APIs with Firefox OS.*

Advantages with hosted web applications compared to packaged web applications

- Content can be dynamically updated without re-installation of application, i.e. all users will always get the latest version
  - User benefit: No re-installation of application needed
  - Service provider benefit:
    - Bug fixes reached out imediately, which is good for brand
    - Frequent content updates and dynamically updated content possible

- Phased launch and A/B testing
  - By designing the back-end delivery infrastructure it is possible to make conscious choices about where and to whom a certain version or incarnation of a specific app is deployed. (For instance, service certain specially tailored apps to certain operators or countries).
  - Additionally it is possible to perform A/B or multivariate tests without users having to download a certain app or version

FFOS API permission levels

SONY
make.believe

- “Web” apps permissions
  - “Web” apps follow the web security model and in general can not gain higher privileges than regular web pages. They may be hosted or packaged, and installed via the Firefox Marketplace, or from any website.
- “Privileged” permissions
  - More sensitive APIs are restricted to “privileged” apps. For actually receiving these permissions, the app must be signed by the Mozilla Marketplace. “Privileged” apps are ZIP files that are digitally signed and distributed from the Mozilla Marketplace. All privileged apps undergo a security review by a (human) reviewer. The application review process is described at the following link: https://developer.mozilla.org/en-US/Marketplace/Publishing/Marketplace_review_criteria
- “Certified” permissions
  - “Certified” permissions give access to system APIs which are needed to build a web-based mobile operating system. For security and/or privacy reasons, these APIs cannot be exposed to either privileged or hosted apps. Certified permissions can only be granted at build time (Gaia apps) and are not available to apps installed by the user (except to side-loaded apps for developers).

FFOS API permission table

- The API permission table defines for each API and permission level the access rights and required user interaction: https://github.com/yinjun/AppManager/blob/master/gecko/dom/apps/src/PermissionsTable.jsm

SoMC FFOS trusted hosted apps

SONY
make.believe

- SoMC is evaluation a model for trusted hosted web applications.
- An additonal permission level, ”trusted”, meaning trusted hosted application, is added.
- Trusted hosted applications are allowed to access more sensitive APIs than normal web sites.

SoMC FFOS trusted hosted apps - description

SONY
make.believe

1. Content and manifest are downloaded to the device with ssl/tls, i.e. server authentication, encryption and integrity protection.
2. Certificate pinning is used, which means that only certain specific certificates are trusted, for example only certificates signed by Sony and Mozilla are trusted.
3. Signature of trusted app's manifest must be verified by a trusted authority
4. There is a CSP field in the manifest file. It is defined so that by default only "self" is allowed, i.e. only content from the origin domain of the app is allowed to download. It is also possible to whitelist other domains with CSP that may be accessed through ssl/tls with certificate pinning. The resources that are accessed through ssl/tls with pinning are script and style src resources. (as declared in 'style-src' and 'script-src' directives in CSP element of the manifest.)

   In addition default security policies apply:
   - Eval and related functions are disabled
   - Inline JavaScript will not be executed
5. Trusted hosted apps are allowed to access a set of more sensitive APIs than normal hosted apps.

SoMC FFOS trusted hosted apps – manifest example

```
{
  "name": ”Test app",
  "description": ”Test of trusted hosted apps",
  "version": "1.0",
  "type": "trusted",
  "launch_path": "/index.html",
  "icons": { "16": "/favicon.ico" },
  "developer”: { "name": ”Developer Team", "url": "http://devloper.com" },
  "csp" : "script-src ’self’ https://.123.testfront.net; style-src 'self’ https://123.testfront.net",
  "permissions": {
    "device-storage:videos":{ "access": "readonly" },
    "device-storage:pictures":{ "access": "readwrite" }
  },
  "appcache_path": "/manifest.appcache"
}
```

SoMC FFOS trusted hosted apps – extended permission table example

```
"device-storage:pictures": {
   app: DENY_ACTION,
   trusted: PROMPT_ACTION,
   privileged: PROMPT_ACTION,
   certified: ALLOW_ACTION,
   access: ["read", "write", "create"]
},

"device-storage:videos": {
   app: DENY_ACTION,
   trusted: PROMPT_ACTION,
   privileged: PROMPT_ACTION,
   certified: ALLOW_ACTION,
   access: ["read", "write", "create"]
},
```

FFOS bug

- https://bugzilla.mozilla.org/show_bug.cgi?id=1016421