Security Model of Firefox OS

Anthony VEREZ[1] Guillaume HUGUES[1]

Soutenance mini-projets SSR, 2013

Table of Contents

History

- Jul 2011 : Announcement

History

- Jul 2011 : Announcement
- Jul 2012 : Alcatel and ZTE become first manufacturers

History

- Jul 2011 : Announcement
- Jul 2012 : Alcatel and ZTE become first manufacturers
- Nov 2012 : First Firefox OS simulator

History

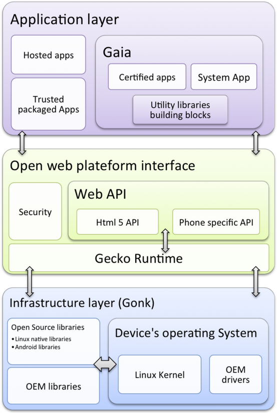
- Jul 2011 : Announcement
- Jul 2012 : Alcatel and ZTE become first manufacturers
- Nov 2012 : First Firefox OS simulator
- Dec 2012 : Version 1.0 of Firefox 0S (stable)

History

- Jul 2011 : Announcement
- Jul 2012 : Alcatel and ZTE become first manufacturers
- Nov 2012 : First Firefox OS simulator
- Dec 2012 : Version 1.0 of Firefox 0S (stable)
- Mar 2013 : Version 1.1.1 of Firefox 0S

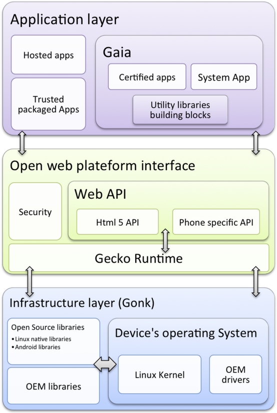
Architecture

- Architecture in 3 layers : Gonk, Gecko, Gaia



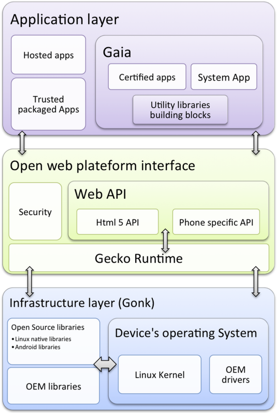
Architecture

- Architecture in 3 layers : Gonk, Gecko, Gaia
- Gonk : The lower-level interface (firmware, Linux kernel, drivers, HAL)



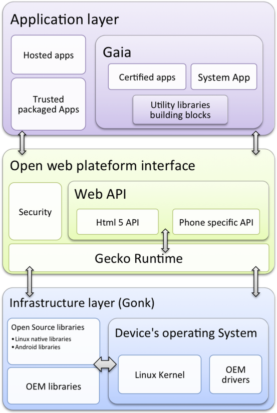
Architecture

- Architecture in 3 layers : Gonk, Gecko, Gaia
- Gonk : The lower-level interface (firmware, Linux kernel, drivers, HAL)
- Gecko : Mozillas layout engine



Architecture

- Architecture in 3 layers : Gonk, Gecko, Gaia
- Gonk : The lower-level interface (firmware, Linux kernel, drivers, HAL)
- Gecko : Mozillas layout engine
- Gaia : The user interface (HTML5 web applications)



Applications

- All apps are HTML5 (HTML5,CSS3,Javascript)

Applications

- All apps are HTML5 (HTML5,CSS3,Javascript)

- App = manifest file + resources

```
{
  "name": "My SSR App",
  "description": "Does nothing...",
  "launch_path": "/",
  "icons": {
    "128": "/img/icon-128.png"
  },
  "developer": {
    "name": "Anthony Verz & Guillaume Hugues",
    "url": "http://www.homepage.com"
  },
  "default_locale": "en",
  "installs_allowed_from": [
    "https://marketplace.firefox.com",
    "https://marketplace.example.com"
  ],
  "orientation": ["portrait"],
  "permissions": {
    "contacts": {
      "description": "Required for ...",
      "access": "readwritecreate"
      },
    "geolocation": {
      "description": "Required for ..."
    }
  }
}
```

Applications

- All apps are HTML5 (HTML5,CSS3,Javascript)

- App = manifest file + resources

- Hosted apps vs. Packaged/Installed apps

```
{
 "name": "My SSR App",
 "description": "Does nothing...",
 "launch_path": "/",
 "icons": {
  "128": "/img/icon-128.png"
 },
 "developer": {
  "name": "Anthony Verz & Guillaume Hugues",
  "url": "http://www.homepage.com"
 },
 "default_locale": "en",
 "installs_allowed_from": [
  "https://marketplace.firefox.com",
  "https://marketplace.example.com"
 ],
 "orientation": ["portrait"],
 "permissions": {
  "contacts": {
   "description": "Required for ...",
   "access": "readwritecreate"
   },
  "geolocation": {
   "description": "Required for ..."
  }
 }
}
```

Applications

- All apps are HTML5 (HTML5,CSS3,Javascript)
- App = manifest file + resources
- Hosted apps vs. Packaged/Installed apps
- Javascript functions divided in separate APIs (Application Programming Interfaces) for security

```
{
  "name": "My SSR App",
  "description": "Does nothing...",
  "launch_path": "/",
  "icons": {
    "128": "/img/icon-128.png"
  },
  "developer": {
    "name": "Anthony Verz & Guillaume Hugues",
    "url": "http://www.homepage.com"
  },
  "default_locale": "en",
  "installs_allowed_from": [
    "https://marketplace.firefox.com",
    "https://marketplace.example.com"
  ],
  "orientation": ["portrait"],
  "permissions": {
    "contacts": {
      "description": "Required for ...",
      "access": "readwritecreate"
      },
    "geolocation": {
      "description": "Required for ..."
    }
  }
}
```

Hardware

- Support for Android 4.0
- Constructors : Alcatel, ZTE, LG, Huawei and Foxconn
- First Firefox OS phones : Alcatel One Touch Fire & ZTE Open

Table of Contents

1. General overview of Firefox OS
2. Security Guidelines
3. Security Implementation
   - User Side
   - Application developpement
   - System architecture
4. Security of Competitors' Products
5. Conclusion

Mechanisms

- Privacy

Mechanisms

- Privacy
- Strict security reviews scheme

Mechanisms

- Privacy
- Strict security reviews scheme
- Apps security : permissions, isolation and code review

Mechanisms

- Privacy
- Strict security reviews scheme
- Apps security : permissions, isolation and code review
- Updates : code signing and network security

Mechanisms

- Privacy
- Strict security reviews scheme
- Apps security : permissions, isolation and code review
- Updates : code signing and network security
- Memory corruption protections

Mechanisms

- Privacy
- Strict security reviews scheme
- Apps security : permissions, isolation and code review
- Updates : code signing and network security
- Memory corruption protections
- File system hardening

Mechanisms

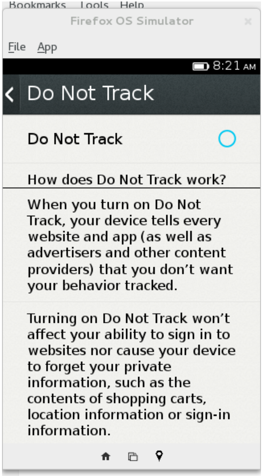
- Privacy
- Strict security reviews scheme
- Apps security : permissions, isolation and code review
- Updates : code signing and network security
- Memory corruption protections
- File system hardening

- Divided in 3 role points of view
  - User side
  - Application developpement
  - System architecture

Table of Contents

1. General overview of Firefox OS
2. Security Guidelines
3. Security Implementation
    - User Side
    - Application developpement
    - System architecture
4. Security of Competitors' Products
5. Conclusion

Settings



Do Not Track

Do Not Track ○

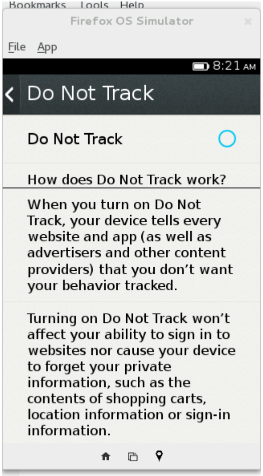
How does Do Not Track work?

When you turn on Do Not Track, your device tells every website and app (as well as advertisers and other content providers) that you don't want your behavior tracked.

Turning on Do Not Track won't affect your ability to sign in to websites nor cause your device to forget your private information, such as the contents of shopping carts, location information or sign-in information.

- Some apps require user approval before using some APIs

Settings



Do Not Track

Do Not Track ○

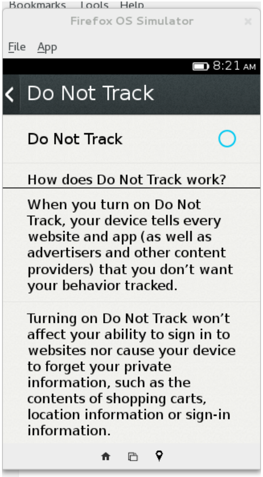
How does Do Not Track work?

When you turn on Do Not Track, your device tells every website and app (as well as advertisers and other content providers) that you don't want your behavior tracked.

Turning on Do Not Track won't affect your ability to sign in to websites nor cause your device to forget your private information, such as the contents of shopping carts, location information or sign-in information.

- Some apps require user approval before using some APIs
- User settings for an app can be changed and authorizations revoked.

Settings



Do Not Track

Do Not Track ○

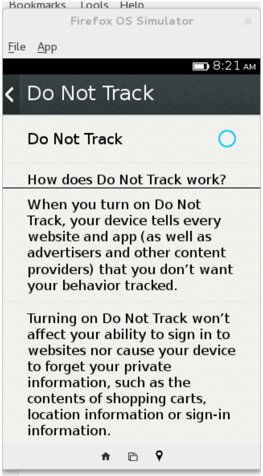
How does Do Not Track work?

When you turn on Do Not Track, your device tells every website and app (as well as advertisers and other content providers) that you don't want your behavior tracked.

Turning on Do Not Track won't affect your ability to sign in to websites nor cause your device to forget your private information, such as the contents of shopping carts, location information or sign-in information.

- Some apps require user approval before using some APIs
- User settings for an app can be changed and authorizations revoked.
- Strong emphasis on privacy

Settings



Do Not Track

Do Not Track ○

How does Do Not Track work?

When you turn on Do Not Track, your device tells every website and app (as well as advertisers and other content providers) that you don't want your behavior tracked.

Turning on Do Not Track won't affect your ability to sign in to websites nor cause your device to forget your private information, such as the contents of shopping carts, location information or sign-in information.

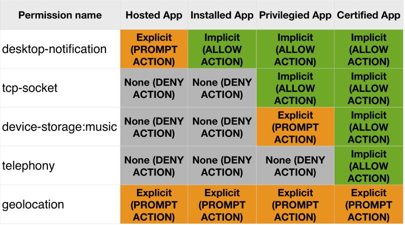
- Some apps require user approval before using some APIs
- User settings for an app can be changed and authorizations revoked.
- Strong emphasis on privacy
- But : Level of configuration very light

App permissions

- Packaged = Normal, Privileged, Certified

App permissions

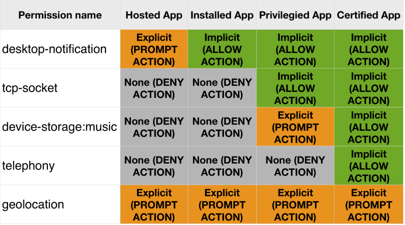
- Packaged = Normal, Privileged, Certified
- Each kind of app has its own matrix of permissions
- Certified apps have implicit ALLOW rights for almost all APIs
- Hosted apps have implicit DENY rights for almost all APIs



Permission name	Hosted App	Installed App	Privilegied App	Certified App
desktop-notification	Explicit (PROMPT ACTION)	Implicit (ALLOW ACTION)	Implicit (ALLOW ACTION)	Implicit (ALLOW ACTION)
tcp-socket	None (DENY ACTION)	None (DENY ACTION)	Implicit (ALLOW ACTION)	Implicit (ALLOW ACTION)
device-storage:music	None (DENY ACTION)	None (DENY ACTION)	Explicit (PROMPT ACTION)	Implicit (ALLOW ACTION)
telephony	None (DENY ACTION)	None (DENY ACTION)	None (DENY ACTION)	Implicit (ALLOW ACTION)
geolocation	Explicit (PROMPT ACTION)	Explicit (PROMPT ACTION)	Explicit (PROMPT ACTION)	Explicit (PROMPT ACTION)

App permissions

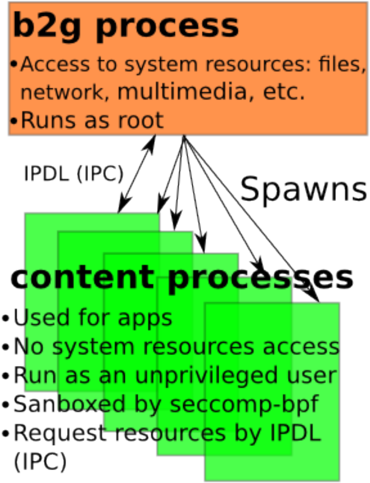
- Packaged = Normal, Privileged, Certified
- Each kind of app has its own matrix of permissions
- Certified apps have implicit ALLOW rights for almost all APIs
- Hosted apps have implicit DENY rights for almost all APIs



Permission name	Hosted App	Installed App	Privilegied App	Certified App
desktop-notification	Explicit (PROMPT ACTION)	Implicit (ALLOW ACTION)	Implicit (ALLOW ACTION)	Implicit (ALLOW ACTION)
tcp-socket	None (DENY ACTION)	None (DENY ACTION)	Implicit (ALLOW ACTION)	Implicit (ALLOW ACTION)
device-storage:music	None (DENY ACTION)	None (DENY ACTION)	Explicit (PROMPT ACTION)	Implicit (ALLOW ACTION)
telephony	None (DENY ACTION)	None (DENY ACTION)	None (DENY ACTION)	Implicit (ALLOW ACTION)
geolocation	Explicit (PROMPT ACTION)	Explicit (PROMPT ACTION)	Explicit (PROMPT ACTION)	Explicit (PROMPT ACTION)

- Authorization must be requested in manifest file

b2g and content processes



b2g process

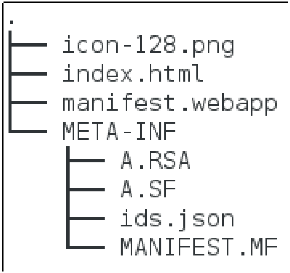
- Access to system resources: files, network, multimedia, etc.
- Runs as root

content processes

- Used for apps
- No system resources access
- Run as an unprivileged user
- Sanboxed by seccomp-bpf
- Request resources by IPDL (IPC)

App signing for packaged apps

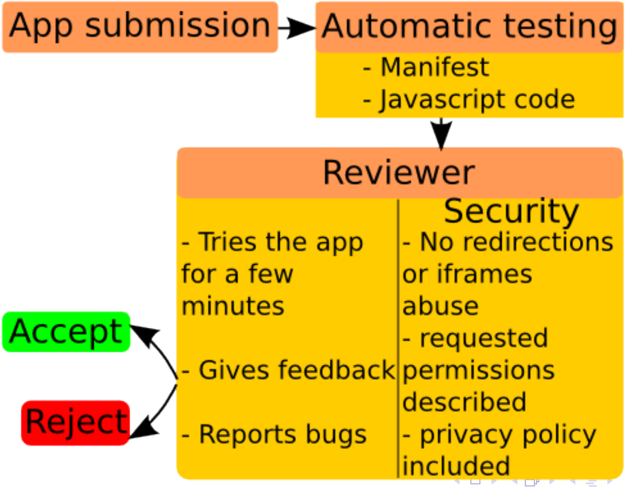
- Goals: integrity, non-repudiation of the developer and ensure that the app has been reviewed
- Cryptographic functions of Firefox (SHA-1, PKCS #7)
- Security of maketplaces not run by Mozilla?
- Patches for updates developed but not integrated into the main codebase yet



```
.
├── icon-128.png
├── index.html
├── manifest.webapp
└── META-INF
    ├── A.RSA
    ├── A.SF
    ├── ids.json
    └── MANIFEST.MF
```

Figure : my_signed_app.zip

App validation



App submission

Automatic testing
- Manifest
- Javascript code

Reviewer

- Tries the app for a few minutes
- Gives feedback
- Reports bugs

Security
- No redirections or iframes abuse
- requested permissions described
- privacy policy included

Accept

Reject

Sandboxing

- “confining a helper application to a restricted environment, within which it has free reign.”

Sandboxing

- "confining a helper application to a restricted environment, within which it has free reign."
- **IPC**: Inter-Process Communications. Each app has its own process (content process) with its workspace and resources.
  - cookies
  - databases
  - offline storage
  - etc.

Sandboxing

- "confining a helper application to a restricted environment, within which it has free reign."
- **IPC**: Inter-Process Communications. Each app has its own process (content process) with its workspace and resources.
  - cookies
  - databases
  - offline storage
  - etc.
- **Seccomp-bpf** to sandbox system calls (e.g., exit, read or write functions)

Address Space Layout Randomization (ASLR)

Randomizing memory space layouts to prevent memory corruption

First run of the "cat" program on Linux 64 bits (simplified)

Start Address	End Address	Label
00400000	0040b000	/usr/bin/cat
012b1000	012d2000	heap
7f144b0fa000	7f144b29d000	/usr/lib/libc-2.17.so
7fff9c2e1000	7fff9c302000	stack

Second run

Start Address	End Address	Label
00400000	0040b000	/usr/bin/cat
0141d000	0143e000	heap
7fb4ed9fe000	7fb4edba1000	/usr/lib/libc-2.17.so
7fff0a408000	7fff0a429000	stack

File system hardening (1)

- Goals: prevent information leaks, privilege escalation and execution of native code
- Give read-write rights only to areas with user content
- File system hardening is based on Android

File system hardening (2)

Mount point	File system	Options
/	rootfs	read-only
/dev	tmpfs	read-write, nosuid, noexec, mode=0755
/proc	proc	read-write, nosuid, nodev, noexec
/cache	yaffs2 or ext4	read-write, nosuid, nodev, noexec
/system	ext4	read-only, nodev
/data	ext4	read-write, nosuid, nodev, noexec
/mnt/sdcard	ext4 or vfat	read-write, nosuid, nodev, noexec, uid=1000, fmask=0702, dmask=0702

Table : (Simplified) Filesystem Mounts

Table of Contents

1. General overview of Firefox OS
2. Security Guidelines
3. Security Implementation
   - User Side
   - Application developpement
   - System architecture
4. Security of Competitors' Products
5. Conclusion

Android

- Most used mobile operating system in Q1 2013 (75%)
- Most targeted by malware (used to be very stupid)

Android

- Most used mobile operating system in Q1 2013 (75%)
- Most targeted by malware (used to be very stupid)
- Main security layers similar to those of Firefox OS

Android

- Most used mobile operating system in Q1 2013 (75%)
- Most targeted by malware (used to be very stupid)
- Main security layers similar to those of Firefox OS
- Application sandbox creates a user/process for each app/library

Android

- Most used mobile operating system in Q1 2013 (75%)
- Most targeted by malware (used to be very stupid)
- Main security layers similar to those of Firefox OS
- Application sandbox creates a user/process for each app/library
- Better memory corruption mitigation than Firefox OS

Android

- Most used mobile operating system in Q1 2013 (75%)
- Most targeted by malware (used to be very stupid)
- Main security layers similar to those of Firefox OS
- Application sandbox creates a user/process for each app/library
- Better memory corruption mitigation than Firefox OS
- Security Vendors

Android

- Most used mobile operating system in Q1 2013 (75%)
- Most targeted by malware (used to be very stupid)
- Main security layers similar to those of Firefox OS
- Application sandbox creates a user/process for each app/library
- Better memory corruption mitigation than Firefox OS
- Security Vendors
- Difficult to upgrade Android on a device

iOS

- A lot of security features enabled by default: boot chain, code signing, advanced memory corruption mitigation, file system hardening and sandboxing

iOS

- A lot of security features enabled by default: boot chain, code signing, advanced memory corruption mitigation, file system hardening and sandboxing
- But a jailbreak is released as soon as a new iOS version is out

iOS

- A lot of security features enabled by default: boot chain, code signing, advanced memory corruption mitigation, file system hardening and sandboxing
- But a jailbreak is released as soon as a new iOS version is out
- Limited malware due to strict restriction of the App Store
- Reduced attack surface due to external software

Blackberry

- Security is a strong marketing argument

Blackberry

- Security is a strong marketing argument
- Robust cryptography
- QNX Kernel: a process manager for each process prevents memory corruption

Blackberry

- Security is a strong marketing argument
- Robust cryptography
- QNX Kernel: a process manager for each process prevents memory corruption
- Blackberry Enterprise Server in companies, for confidentiality and ensure security compliance

Blackberry

- Security is a strong marketing argument
- Robust cryptography
- QNX Kernel: a process manager for each process prevents memory corruption
- Blackberry Enterprise Server in companies, for confidentiality and ensure security compliance
- In May 2013, Blackberry 10 first mobile platform approved by the U.S. DoD for future agency use

Table of Contents

1 General overview of Firefox OS

2 Security Guidelines

3 Security Implementation
- User Side
- Application developpement
- System architecture

4 Security of Competitors' Products

5 Conclusion

Conclusion

- Delay but most crucial security features are here

Conclusion

- Delay but most crucial security features are here
- Security guidelines often inherited from Android

Conclusion

- Delay but most crucial security features are here
- Security guidelines often inherited from Android
- Openness and performance vs security

Conclusion

- Delay but most crucial security features are here
- Security guidelines often inherited from Android
- Openness and performance vs security
- No Java or native code code but web technologies: magnified web attacks?