NetFront Widgets

Security Model

W3C Mobile Web Initiative

10-11 December 2008

Marcin Hanclik

2008.12.10

ACCESS™

Open Up Your World

NetFront Widgets (NFW)

- Based on W3C specifications
  - Widgets 1.0 Digital Signature
  - Widgets 1.0 Packaging&Configuration
- Browser vs. Widgets Player
- Security Model
  - Same Origin Policy
  - Network access restrictions
  - JavaScript API access restrictions
- Security model that already works

ACCESS™

Open Up Your World

NFW - Browser vs. Widgets Player

- Disabled functions of DOM objects:
  - Pop-ups: alert(), confirm(), prompt()
  - Navigation: back(), forward(), go(), home()
  - Document stream handling: open(), close()
- `referrer` property is not set for local content (widget URI)
- No concept of „visits” results in disabling:
  - Coloring visited links using `vlink` attribute of body element
  - Changing style of visited links using `:visited` pseudo class of CSS

ACCESS™

Open Up Your World

NFW – Page Transition Behavior

	Internal URI (`widget://`)	External URI
Anchor selection	Page transition (the query part of the URI is deleted)	Launch of the external application
Form submission	Ignored	Ignored for top level window, page transition for frame/iframe element
Rewriting `location.href`	Page transition	Lanch of the external application
Rewriting `src` attribute of the `frame/iframe` element	Page transition (the query part of the URI is deleted)	Page transition (`<netaccess>` takes care of security)

ACCESS™

Open Up Your World

NFW Security Model – - Same Origin Policy

- Origins identified by „domain”
  - URI scheme
  - Host name
  - Port number
- Same Origin Policy is relaxed and is **NOT** applied to **XMLHttpRequest**.

ACCESS™

Open Up Your World

NFW Security Model – - Network access restrictions

- Specified in `config.xml`
- `<access>` element
  - `network` attribute
  - Boolean value for generic network access
- `<netaccess>` element
  - `host` attribute
  - `port` attribute
  - Host and port pairs enabling HTTP access to particular servers
  - E.g.: <netaccess port="80,100,101,1000-2000" />

ACCESS™

Open Up Your World

NFW Security Model – - JavaScript API access restrictions

- Based on MIDP2.0
- Terms
  - Protection domain
    - A logical unit used to define access permission settings for a function group.
  - Function group
    - Defines a group of JavaScript object properties to be protected.
  - Permission
    - allow
    - session
    - oneshot (usability aspects!)
    - prohibit
- Restrictions are specified in **Policy Definition File**

ACCESS™

Open Up Your World

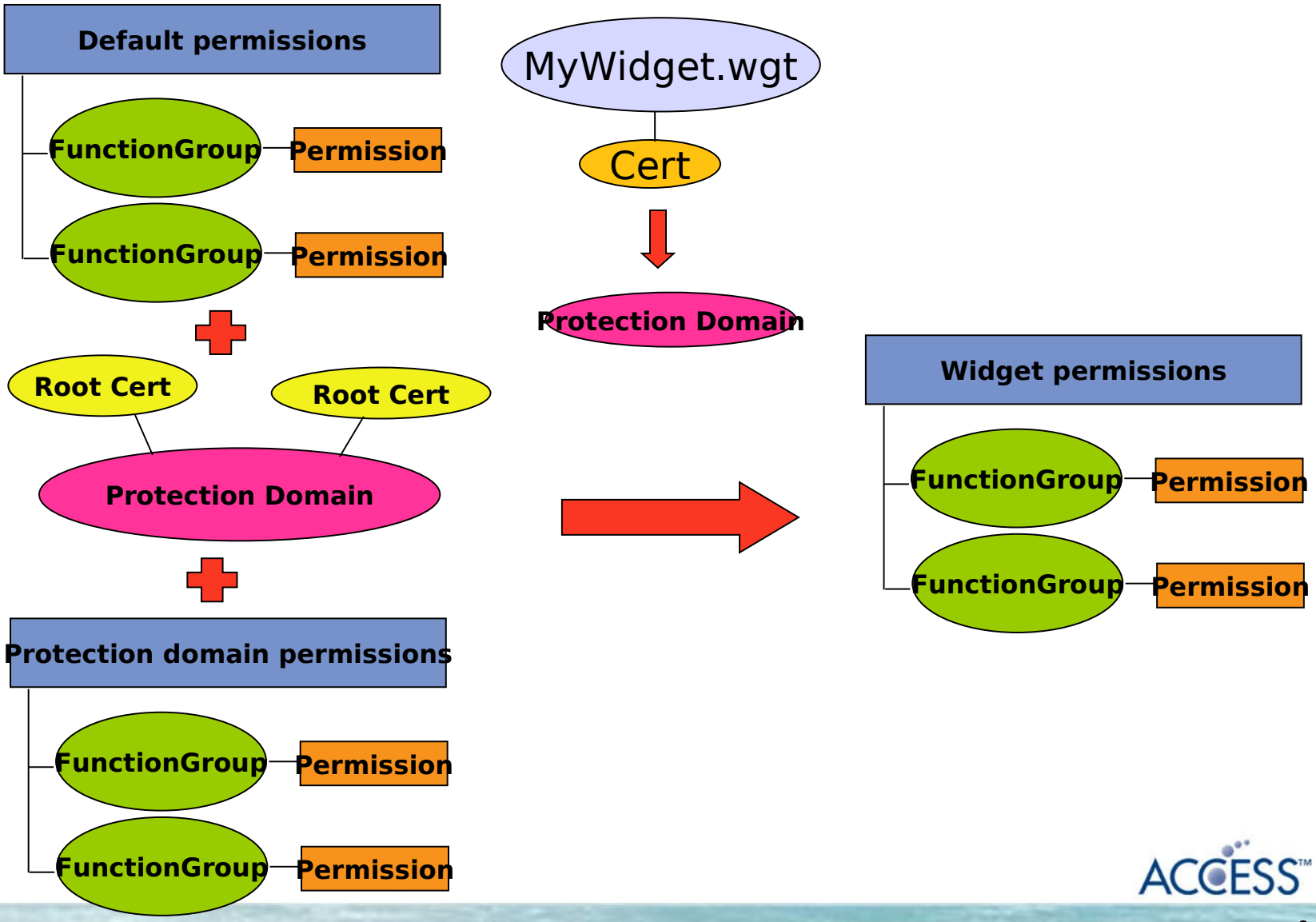
NFW Security Model – - Trust model

- NFW Security Model
  - Provides access to sensitive functionalities only for authenticated widgets
  - Does not specify how policy is delivered to the terminal, but is open to any delivery method (OMA DM is preferred in BONDI).
- NFW Trust Model definition is thus defined during the integration of NFW within the device
  - By Operator
  - By Device Vendor
  - By End User
- Web applications do not have access to device APIs

ACCESS™

Open Up Your World

NFW Security Model –
- How permissions work, simple model



Open Up Your World

NFW Security Model – - Post-installation processes

- Black list look up
  - Detection of malware prior to installation may be inperfect
- Forgery detection
  - Periodic widget re-validation

ACCESS™

Open Up Your World

NFW – Remarks

- Having one, simple standard is of great value for all market players, including users and developers
- BONDI Interfaces implemented partially
- More at http://widgets.access-company.com
- NFW has been deployed at DoCoMo, Softbank

ACCESS™

Open Up Your World

Thank you!