WebOS Security

WebOS Developers Workshop Mainz

21.04.2012

Author: Pablo Endres

Agenda

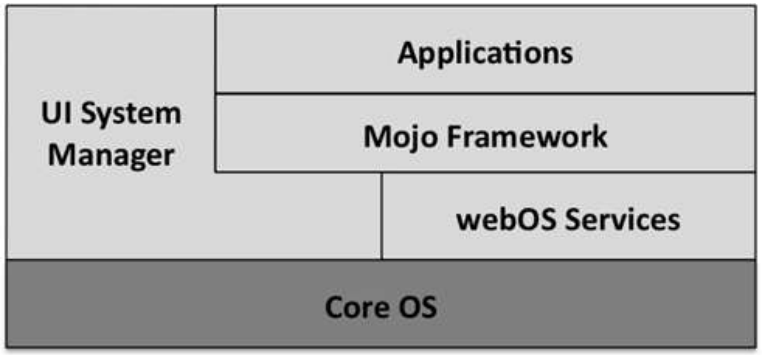
- Architecture
- OS / Platform
- Authentication
- Networking
- Browser
- Email
- PIM
- MDM
- Other

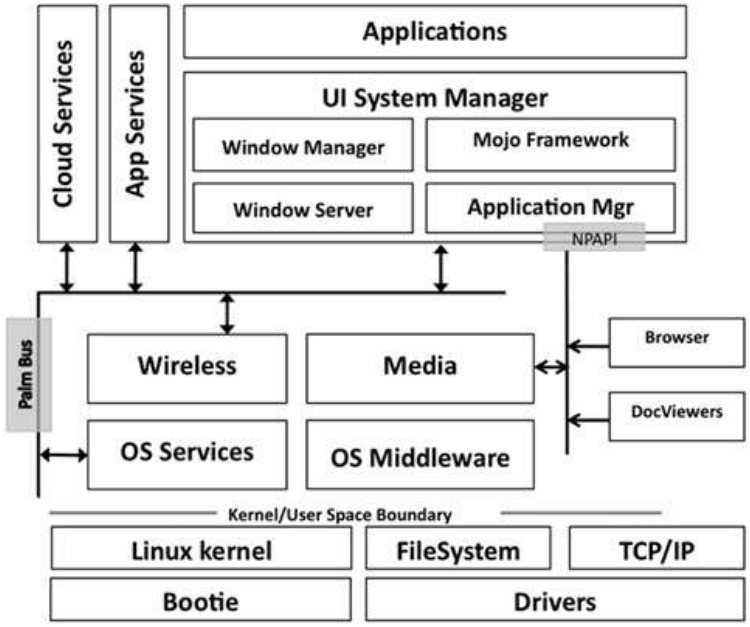
WebOS Security

Architecture

WebOS Security

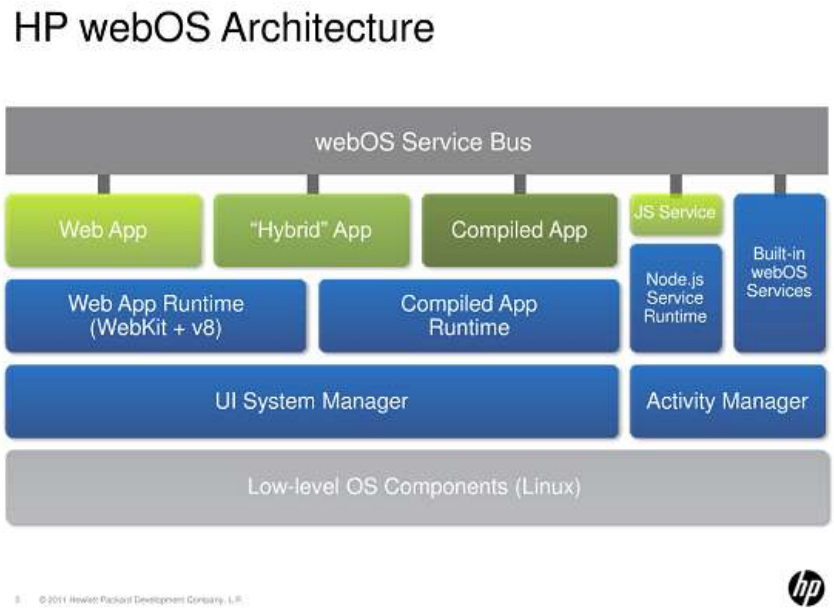
- WebOS is a Platform
- OS:2.6 Linux kernel
- All interactions with the framework
  - 1.x and 2.x Mojo
  - 3.x Enyo
    - No architecture on the web
      -> Assume simple exchange





WebOS Security

- All Web Apps run with the same user
  - No permission mgmt
  - Access to cookies
  - Possible cross pollination
  - Possible traffic injection
- Jail roots exist for Hybrid and Compiled Apps
  - /usr/bin/jailer
  - /etc/jail_default.conf



WebOS Security

FILE SYSTEM SECURITY

- Makes use of LVM
  - Easy to restructure without loss

```
lvm> lvs
  LV         VG    Attr   LSize   …
  cm-cache   store -wi-a- 200.00M
  cm-data    store -wi-a-   1.50G
  cm-system  store -wi-a- 304.00M
  filecache  store -wimao 136.00M
  log        store -wimao  24.00M
  media      store -wimao  25.63G
  mojodb     store -wimao 256.00M
  root       store -wimao 568.00M
  swap       store -wimao 400.00M
  update     store -wima-  16.00M
  var        store -wimao  64.00M
```

- File systems used
  - EXT3
  - VFAT

- Encryption
  - Based on LUKS + dm-crypt
  - /etc/cryptofs.conf -> configuration

```
[CryptoFS]
cipher=BLOWFISH
md=MD5
blocksize=4096
salts=1
```

- Encrypted FS
  - /dev/mapper/store-filecache
  - /dev/mapper/store-mojodb
- Encryption keys:
  - /var/palm/data/store-cryptodb.key
  - /var/palm/data/store-cryptofilecache.key

WebOS Security

PASSWORD MANAGEMENT

- Managed and stored by the *keymanager*
- Supports
  - AES-128, AES-192, AES-256, DES/3DES
  - HMAC / SHA1
- API checks for owner of the keys (APP)
- If used correctly should be non-reversable

KEY MANAGER

- SQLite 3.x database
- /var/palm/data/keys.db
- Can also be copied out of /proc

```
sqlite3 /var/palm/data/keys.db
sqlite> .schema
CREATE TABLE keytable(id INTEGER
    PRIMARY KEY,ownerID TEXT,keyID
    TEXT,data BLOB,keysize INTEGER,type
    INTEGER,scope INTEGER, hash BLOB);

CREATE TABLE keytableconfig(id INTEGER
    PRIMARY KEY,data BLOB,dataLength
    INTEGER,iv BLOB,ivLength INTEGER);
```

WebOS Security

MONITORING

- **Can be read in clear-text by using ls-monitor**
  - **Works only when changing passwords**

```
196811.105          [PRV]      call       11                    (null) (/var/run/ls2/FlUAw3)
         com.palm.keymanager (/var/run/ls2/D52L6L)             (null)
         //changePassword      «{ "oldPassword": "c0mPlexpa$$wd!", "newPassword": "qw" }»
```

WebOS Security

CAMERA & MIC

(Work in progress)

- No support in the API in 1.x and 2.x
- 3.X API enables access to camera and audio
- No permission mgmt -> Any APP can activate it without warning

Authentication

WebOS Security

- Types of authentication: PIN / Password
  - Must be at least 1 digit/char long
  - No complexity rules -> missing options -> APP / Patch
  - According to white paper this is supported with EAS
- Max number of failed password attempts
  - Brute-force / dictionary attacks possible
    - Nothing happens after 30 failed attempts
  - No exponential back-off or timeout
  - No option to wipe after X failed attempts
- Auto lock: yes
  - Min 30 sec. - max 30 min
- Remote wipe (I haven't tried them yet)
  - Via palm profile
  - Via ActiveSync / Exchange -> Yes according to the security white paper

WebOS Security

(Work in progress)

- Wi-Fi
  - Only WPA2 and EAP
- Portscans
  - No open ports by default
  - SSH -> uses keys by default
- VPN
  - Cisco AnyConnect (SSL)
  - VPNC (IPSec)
  - OpenVPN (homebrew or opware)
- Bluetooth
  - Supported profiles
    - HFP/HSP
    - A2DP
    - AVRCP
    - OPP
    - SPP
    - MAP
    - HID
  - Secure authentication is preferred
- Clear-text traffic
  - Non has been observed until now

Browser

WebOS Security

- http://bcheck.scanit.be/
  - is gone
- https://browsercheck.qualys.com
  - Qualys doesn't support the browser
- http://www.browserscope.org/

1. PASS postMessage API
2. PASS JSON.parse API
3. FAIL toStaticHTML API
4. FAIL httpOnly cookie API
5. PASS X-Frame-Options
6. FAIL X-Content-Type-Options
7. FAIL Block reflected XSS
8. PASS Block location spoofing
9. PASS Block JSON hijacking
10. PASS Block XSS in CSS
11. FAIL Sandbox attribute
12. PASS Origin header
13. FAIL Strict Transport Security
14. PASS Block cross-origin CSS attacks
15. FAIL Content Security Policy
16. PASS Cross Origin Resource Sharing
17. PASS Block visited link sniffing

WebOS Security

E-mail

- Providers out of the box:
  - Email: POP, IMAP, EAS
  - Google
  - Exchange
  - Mobile Me
  - Yahoo!
- Use of encrypted protocols by default on Synergy providers
- No spam filter
- No anti-virus protection
- Attachments can be sent
- Supports exchange policies (EAS)
  - According to whitepaper
  - I haven't tested them myself

WebOS Security

PIM

- Synergy does not mix account information

MDM

- Only Exchange is supported via EAS
- Haven't performed any tests with this

PACKAGE MANAGERS

- 3 different ipkg databases
  - `system /usr/lib/ipkg`
  - `preware /media/cryptofs/usr/lib/ipkg/info`
  - `optware (ipkg-opt) /opt/lib/ipkg/info`

WebOS Security

Thank you

Comments / Feedback:
Pablo Endres
@epablosensei
http://www.PabloEndres.com