Putting Device API Privacy and Policy into User Context

Frederick Hirsch

4 October 2010

New DAP APIs; Increased Attack Surface

Contacts (reading from addressbook) / Contacts Writer (writing to addressbook)

```
// Perform an address book search. Obtain the 'name' and 'emails' properties
// and initially filter the list to Contact records containing 'Bob':
navigator.service.contacts.find(['name', 'emails'],.., {filter: 'Bob'});
```

```
// Add new phone number:  myContact.phoneNumbers.push({type: 'home', value: '+440000000002'});
// Update existing contact: myContact.save(successContactCallback, generalErrorCB);
```

Calendar

```
// Remove existing contact: myContact.remove(successContactCallback, generalErrorCB);
```

```
// edit the calendar event location: myEvent.location = 'Conf call number change: #XXX';
// Update an existing calendar event:  myEvent.save(successCalendarEventCallback, gErrorCB);
```

HTML Media Capture (camera/microphone interactions through HTML forms)

```
<input type="file" accept="image/*;capture=camera" id="capture">
```

Media Capture API (programmatic access to camera/microphone)

```
navigator.device.capture.captureImage(success, error, { limit: 1 });
```

Messaging (SMS, MMS, emails)

```
navigator.device.messaging.createSMS({to: [{'+460000000001'}], body: "Hi!"}).send(successCB, eCB);
```

Systems info and events (CPU, network, etc.)

```
//Monitor and display the CPU load:  navigator.system.watch("Processing",success);
```

There are more APIs than just in DAP WG...

Geolocation (determining geographical position information)

```
function showMap(position) {
      // Show a map centered at (position.coords.latitude,position.coords.longitude).
    }
    // One-shot position request.
    navigator.geolocation.getCurrentPosition(showMap);
```

```
// Request repeated updates.
    var watchId = navigator.geolocation.watchPosition(scrollMap);
```

"User agents must not send location information to Web sites without the express permission of the user." http://www.w3.org/2008/geolocation/

File API/File API: Writer (read and write files)

```
var file = document.getElementById('file').files[0]; var reader = new FileReader();
// Read file into memory as UTF-16
reader.readAsText(readFile, "UTF-16");
```

```
var bb = new BlobBuilder();
bb.append("Lorem ipsum");
var fileSaver = window.saveAs(bb.getBlob(), "test_file");
fileSaver.onwriteend = myOnWriteEnd;
```

"This specification also assumes that the primary user interaction is with the <input type="file"/> element of HTML forms [HTML5], and that all files that are being read by FileReader objects have first been selected by the user."

http://dev.w3.org/2006/webapi/FileAPI/ http://dev.w3.org/2009/dap/file-system/file-writer.html

Note: Details are subject to change.

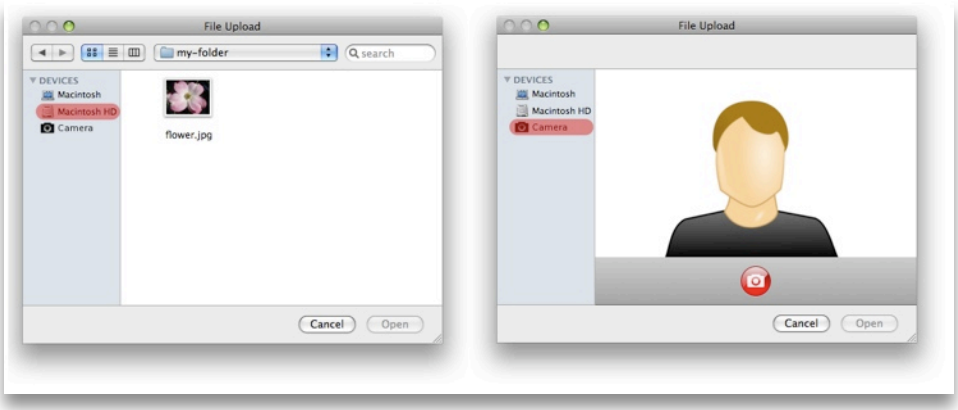
Authorization in User Context

- User-Directed Action
  - Granular User Consent
  - Avoid unnecessary and ineffective prompting & Non-modal dialogs
  - Consent is part of meaningful action
- User-Installed Applications
  - Grouped and retained permissions
  - User decision based application source trust - identity, reputation, context
- User-Delegated-Authority
  - Third-party rules to determine authorization
  - Implies trusted party able to make and deploy rules
    - Possibly difficult in general web context

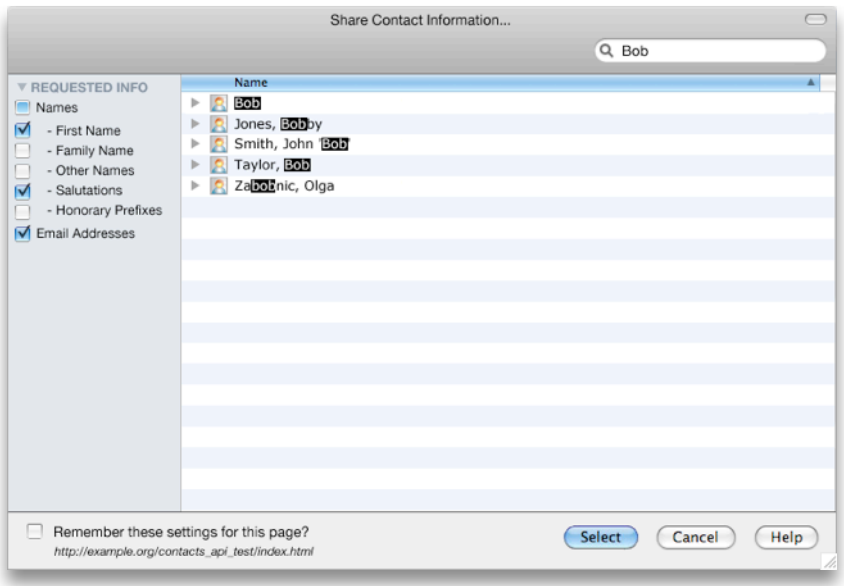
Device API Access Control Use Cases and Requirements http://dev.w3.org/2009/dap/policy-reqs/

User selections - understandable consent

- No user action - nothing happens.
- Choosing items to work with implies consent for those items and action



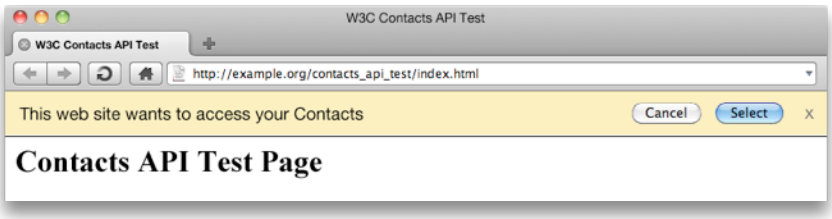
http://www.w3.org/TR/2010/WD-html-media-capture-20100928/



http://www.w3.org/TR/2010/WD-contacts-api-20100817/

Context-specific dialogs for user consent

- Dialogs that fit work flow
  - If ignored - nothing happens
  - When selected, implies consent



http://www.w3.org/TR/2010/WD-contacts-api-20100817/

Applications

- "Install" web application
  - Implies granting multiple permissions at once
  - Possibly implies granting for period of time.
- Not just W3C Widgets but also web applications.

Policy

- Define Permissions http://dev.w3.org/2009/dap/api-perms/
  - Examples: `geolocation` `contacts.read`, `file.read`, `file.write`
  - Work in progress to define permissions at correct granularity
- Define Trust Framework
  - Contributions from Nokia and BONDI
  - Base permissions on trust domains
- Define Policy Markup
- Operational aspects (Out of DAP scope yet essential)
  - Establish trust (via PKI mechanisms, reputation etc)
  - Provisioning

Policy Markup examples

XML to define permissions based on domains

```
<domain name="Untrusted">
  <capability name="UserDataGroup"/>
</domain>
<domain name="OperatorSigned">
  <capability name="UserDataGroup"/>
  <capability name="NetworkGroup"/>
  <capability name="DeviceResourcesGroup"/>
  <capability name="Location"/>
</domain>
```

XACML or XACML-like languages

```
<condition combine="or">
  <resource-match attr="dev-cap" match="messaging.*.send"
        param:recipients="+4409*" func="glob"/> <-- to block UK premium rate numbers -->
  <resource-match attr="dev-cap"
    match="messaging.*.send" param:recipients="+34806*" func="glob"/>
    <-- to block Spanish premium rate numbers -->
</condition>
```

Choice of markup subsequent to framework and other decisions.

Privacy

- Access control and security important but not enough.
- Issues related to data reuse, retention etc.
- RuleSet proposal under consideration in DAP:
  - Simplicity and usability, analogous to Creative Commons licensing
  - Focus on three main parameters: sharing, secondary use, and retention
  - Users attach a rule-set to personal information as they disclose it to the Web site
  - Practical and pragmatic - enables business cases while raising privacy bar
  - Presented at W3C Privacy Workshop July 2010:
    - Paper: http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html
    - Slides: http://www.w3.org/2010/api-privacy-ws/slides/cooper.pdf
  - DAP Draft: http://dev.w3.org/2009/dap/privacy-rulesets/
- Open question: to be agnostic at Browser level or not?

For more information

- DAP publications and roadmap:
  - http://www.w3.org/2009/dap/
- W3C Web Apps WG
  - http://www.w3.org/2008/webapps/wiki/Main_Page
- W3C Geolocation WG
  - http://www.w3.org/2008/geolocation/
- July 2010 W3C Privacy workshop
  - http://www.w3.org/2010/api-privacy-ws/report.html