Trust & Permissions for the Open Web Platform

Break-out Session

Dave Raggett <dsr@w3.org>

29 October 2014

Trust & Permissions

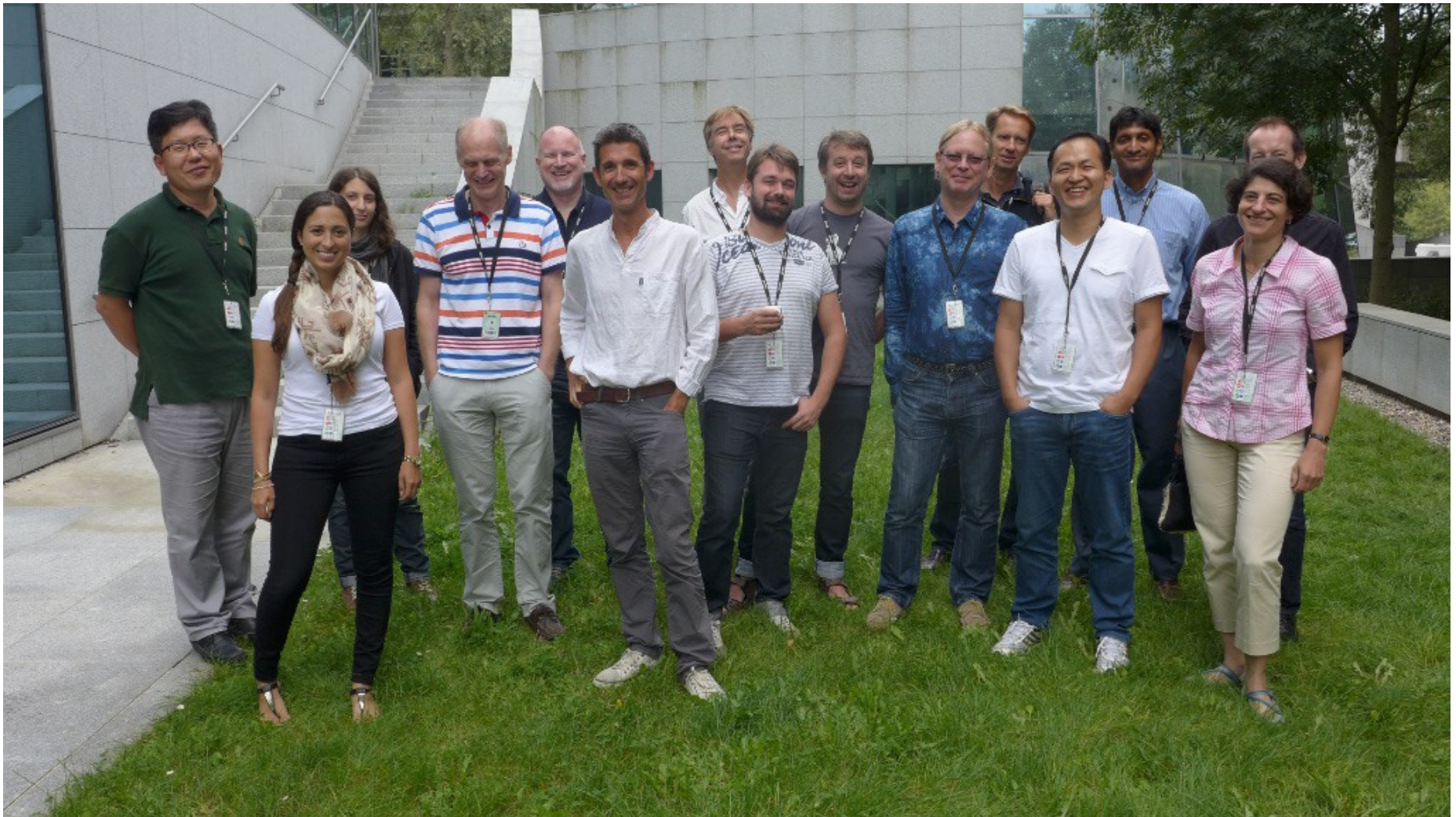
- Apps need to be trusted before they can be given permission to use certain capabilities
  - Capabilities involving access to personal information
    - e.g. location, contacts, local files, camera, microphone
  - Capabilities that if misused could harm the user
    - e.g. payments, raw sockets
- Common approaches include
  - Ask for user consent when app is installed
    - e.g. Android
  - Ask for user consent when capability is used
    - e.g. iOS
  - Browser silently grants permission to platform apps
    - System apps provided by platform vendor
  - Trusted UI for where user intention is clear

Trust & Permissions

Paris, 3-4 September 2014

http://www.w3.org/2014/07/permissions/

Meeting organized by SysApps WG and hosted by Gemalto



Paris meeting

- We shared experiences
  - Native platforms
  - Web platforms
  - Research studies
- And discussed ideas for extending the Open Web Platform
  - But not ruling out packaged apps

- Participants from
  - Apple
  - Ericsson
  - ETRI
  - Gemalto
  - GM
  - Google
  - Intel
  - Microsoft
  - Mozilla
  - Samsung
  - Sony
  - Qualcomm

Next Steps

- General agreement In Paris on launching a W3C Trust and Permissions Community Group
- Focus on best practices and emerging techniques, e.g. trusted UI controls
- Encourage cross WG review of permissions in W3C APIs

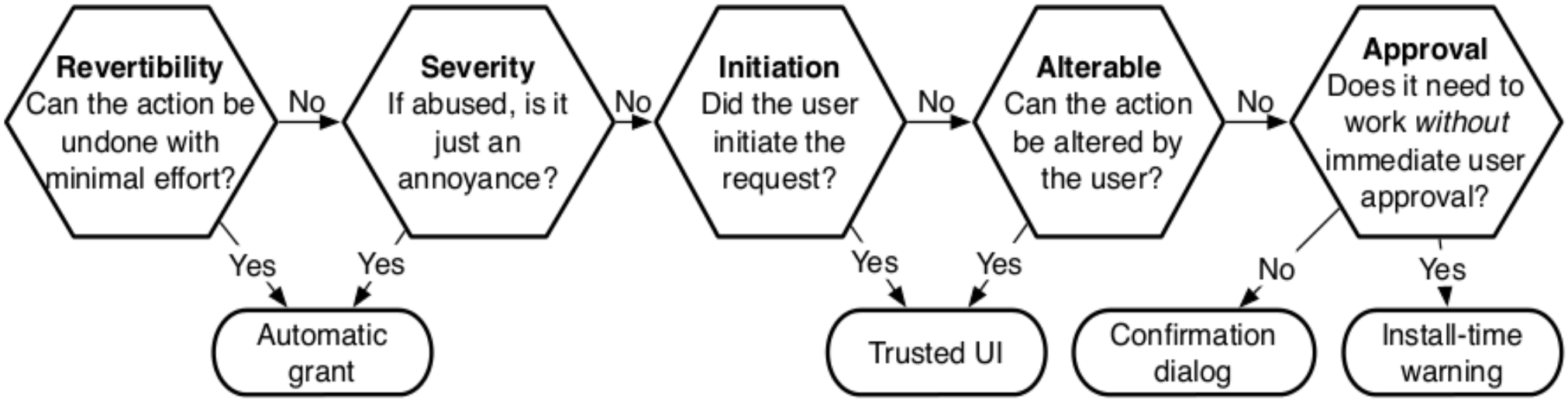
Trust & Permissions

- Agreement that we need shared standards for the Open Web Platform
  - Building on precedents with existing APIs
- The ship has already sailed for packaged apps
  - Entrenched differences across vendor platforms
    - But opportunities for adopting best practices
- Innovation by browser vendors for detecting misbehaving apps
- Increasing role for endorsements by trusted 3rd parties as a way for users to delegate trust decisions

Trust & Permissions

- Native platforms handle this in a proprietary way
  - Apple iOS
  - Google Android
  - Microsoft Windows Phone
- Hybrid platforms subject to host platform
  - Apache Cordova/PhoneGap
- The Open Web Platform (HTML5)
  - Geolocation, Full screen, WebRTC, ...
- Web OS platforms that extend the Open Web Platform in proprietary ways
  - Mozilla Firefox
  - Tizen
  - etc.

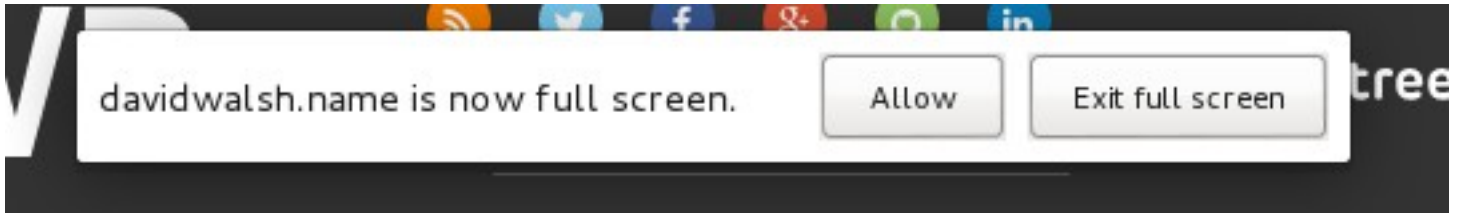
Guidelines



Towards comprehensible and comprehensive permission systems,
Adrienne Felt, Ph.D Dissertation

Automatic Grant

- Full screen API
  - App requests full screen presentation
  - Browser alerts user and allows user to cancel
    - Example UX in Chrome



- Easily undone, and no harm done
  - Browser UI targeted at spoofing attacks

Trusted UI

- Media Capture API
  - HTML form extension that facilitates user access to a device's media capture mechanism, such as a camera, or microphone, from within a file upload control.
- More generally, a means for apps to embed UI controls for specific purposes
  - Controls only work when not occluded in any way
    - And have been so for a minimum time period
  - No or limited ability for app to customize appeance
- Potential HTML5 extension
  - Element linking to HTML fragment (with its own script, style sheet etc.)
    - From 3rd party that user/browser trusts
- More details available in

User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems, Roesner et al. 2011

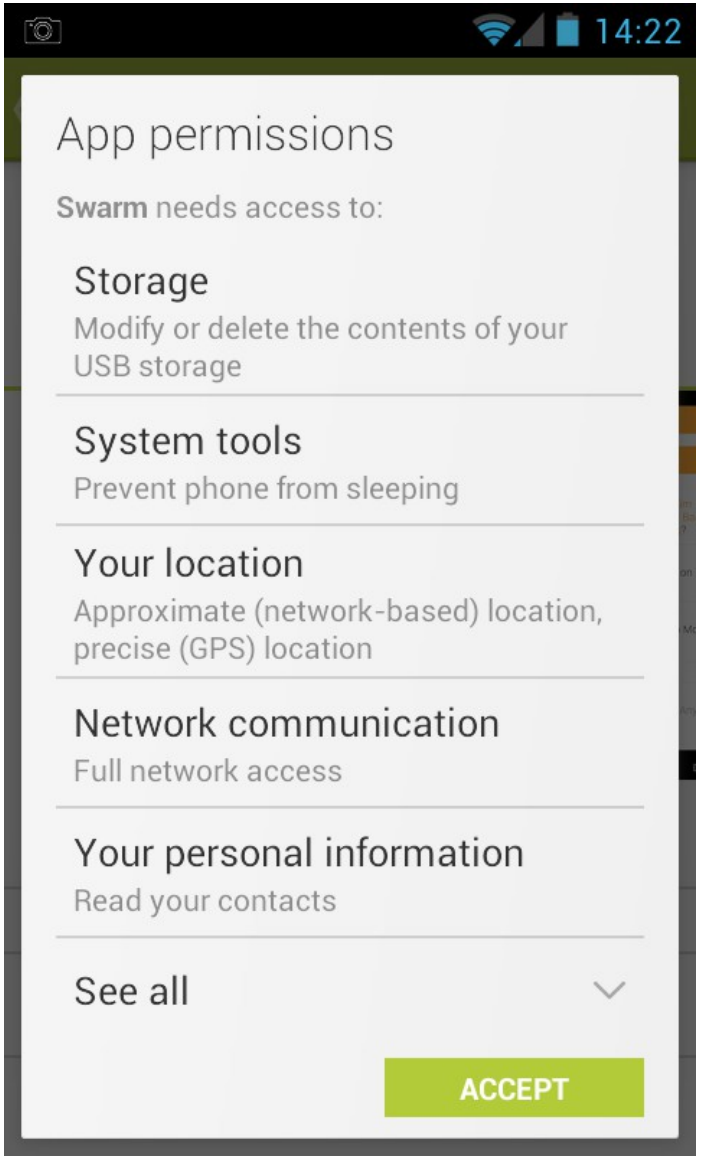
Confirmation Dialog

- Geolocation API
  - Do you want to share your location with this site?

- The action isn't revertible, and shouldn't occur without the user's permission

Install-Time Consent

- When apps wouldn't be able to work without the requested permissions
- But easily abused
  - Users “trained” to tap away the consent dialog
  - Developer's can easily ask for more permissions during updates



Trust Delegation

- App stores may have rigorous processes for vetting apps before allowing users to install them
- Third parties could vet apps for
  - Malware
  - Payware
  - Privacy abuses
- Users can delegate trust so that the browser doesn't need to ask for permission
  - Both at install time and at run-time
- But we need open standard for how hosted apps can cite endorsements

Discussion topics?