User-Centric Permissions for Mobile Devices

Serge Egelman

UC Berkeley
Making security usable

Current problems:

1. Unnecessary interactions *habituate* users
2. Users are asked to make decisions they are unqualified to make

Hazard Avoidance

- Eliminate hazards
- Guard against hazards
- Warn about hazards
Suggestions for Mobile Permissions

Many were habituated—too many requests
Only prompt when necessary

Many were unaware—too late in the process
Provide information earlier

Understanding requires knowing all permissions
Narrow list of possible permissions
THERE CAN BE ONLY ONE?
Permission-granting mechanisms

What are the pros/cons of the various ways of asking for permission?

Previous study looked at install-time warnings, what about other mechanisms?

(Applicable to more than just on smartphones.)
Flowchart

Revertibility
Can the action be undone with minimal effort?

Severity
If abused, is it just an annoyance?

Initiation
Did the user initiate the request?

Alterable
Can the action be altered by the user?

Approval
Does it need to work without immediate user approval?

Yes
No

Yes
No

Yes
No

Yes
No

Implicit access

Trusted UI

Confirmation dialog

Install-time warning

Impact on status quo

Of the 83 permissions...

<table>
<thead>
<tr>
<th>Implicit access</th>
<th>Trusted UI</th>
<th>Runtime</th>
<th>Install-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>55%</td>
<td>23%</td>
<td>16%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Potential to dramatically reduce unnecessary interactions!

Caveat: this does not reflect frequency of use.
Future Work

Human subjects experiments to...

...improve warnings, when they’re needed
...create better audit/notification mechanisms
...validate the system