Context-Specific Access Control

Conforming Permissions With
User Expectations

Amir Rahmati, Harsha V. Madhyastha
Sensitive User Data

- Messages
- Contacts
- Camera
- Emails
- Files
- Location
Access Control Systems
Access Control Systems

Install Time
Access Control Systems

Install Time

First Use
Access Control Systems

Prompt Once

Install Time  First Use
Context Specific Access Control
Context Specific Access Control

Home
Face Recognition
Arrests
Search
Background
Context Specific Access Control

Home  Face Recognition  Arrests  Search  Background
Context Specific Access Control

Camera, Location

Home  Face Recognition  Arrests  Search  Background
Context Specific Access Control
Usability vs. Privacy
Usability vs. Privacy

Prompt Once
Usability vs. Privacy

Usability

Privacy

Prompt Once

Prompt every time
Usability vs. Privacy

- CSAC
- Prompt Once
- Prompt every time
Context-Specific Access Control
Context-Specific Access Control

• **Divide** user’s interaction with application to a limited number of contexts.

• Prompt user for access-control decisions upon first use per-context.

• **Reuse** access-control decisions when user returns to that context.
Context Specific Access Control
Context Specific Access Control

Face Recognition
Context Specific Access Control

Face Recognition

Camera, Location
Context Specific Access Control

Home  Face Recognition  Arrests  Search  Background
Feasibility
Feasibility

- Applications should be modular.
- CSAC decision overhead should be low
Application Modularity
Application Modularity

Median of 6 activities/app
Application Modularity

Activities provide meaningful modularity to implement CSAC
Feasibility

✓ Applications should be modular.

• CSAC decision overhead should be low
Permission Usage

Activity 1
Camera, Location

Activity 2
Camera, Location

Activity 3
Location

Activity 4
Camera, Location

Activity 5
Camera, Location

Activity 6
Camera, Location

Activity 7
Photos
Permission Usage

- Activity 1
- Activity 2
- Activity 3: Location
- Activity 4
- Activity 5: Camera, Location
- Activity 6
- Activity 7: Photos
Experimental Setup
Experimental Setup

• 100 popular free Android applications.
• Dynamic exploration with A3E.
• Tracked use of Camera, Location, Device ID, Bluetooth, and Photos.
Permission usage variation across Activities

![Bar graph showing the number of activities using permissions compared to those not using permissions across applications.](image)
Permission usage variation across Activities

70% of Activities do not use permissions we tracked
Permission Usage

Activity 1
Activity 2
Activity 3
Activity 4
Activity 5
Activity 6
Activity 7

Location
Camera, Location
Photos
Decision Overhead
Decision Overhead
Decision Overhead

![Graph showing decision overhead over applications. The graph compares CSAC and Install time.]
Decision Overhead

For most of the applications CSAC has no overhead.
For most of the applications CSAC has no overhead.
Decision Overhead

For most of the applications CSAC has no overhead.
User Study
User Study

• 5 Applications, 5 Users
User Study

- 5 Applications, 5 Users

<table>
<thead>
<tr>
<th>Application</th>
<th>Dynamic Exploration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Install time</td>
</tr>
<tr>
<td>Dictionary</td>
<td>3</td>
</tr>
<tr>
<td>Flipagram</td>
<td>4</td>
</tr>
<tr>
<td>GasBuddy</td>
<td>3</td>
</tr>
<tr>
<td>WeatherBug</td>
<td>3</td>
</tr>
<tr>
<td>Yelp</td>
<td>4</td>
</tr>
</tbody>
</table>
User Study

- 5 Applications, 5 Users

<table>
<thead>
<tr>
<th>Application</th>
<th>Install time</th>
<th>First use</th>
<th>CSAC</th>
<th>Union</th>
<th>User #1</th>
<th>User #2</th>
<th>User #3</th>
<th>User #4</th>
<th>User #5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>3</td>
<td>2</td>
<td>15</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Flipagram</td>
<td>4</td>
<td>3</td>
<td>8</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GasBuddy</td>
<td>3</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>WeatherBug</td>
<td>3</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Yelp</td>
<td>4</td>
<td>3</td>
<td>15</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
User Study

• 5 Applications, 5 Users

<table>
<thead>
<tr>
<th>Application</th>
<th>Dynamic Exploration</th>
<th>User Study</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Install time</td>
<td>First use</td>
</tr>
<tr>
<td>Dictionary</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Flipagram</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>GasBuddy</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>WeatherBug</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Yelp</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>
Conclusion
Conclusion

• Applications can be broken down to different contexts.

• Different contexts require a different set of permissions.

• CSAC can get us closer to realizing principle of least privilege.

• Many challenges remain: - Data sharing
  - Background services
  - Modifying permissions
Backup Slides
Background vs Foreground

“Weather” has been using your location in the background. Do you want to continue allowing this? Your location is used to show local weather in the "Weather" app and in Notification Center.

<table>
<thead>
<tr>
<th></th>
<th>Settings</th>
<th>Continue</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Google Maps</strong> Would Like to Use Your Current Location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don’t Allow</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>
Context Specific Access Control
Context Specific Access Control
Context Specific Access Control
Context Specific Access Control

Camera,
Location