Context-centric Security

Mohit Tiwari, Prashanth Mohan, Andrew Osheroff, Hilfi Alkaff, Eric Love, Elaine Shi, Dawn Song, Krste Asanović

UC Berkeley
Context-centric Security

• Privacy policies are tied to users’ real-life contexts
  – a conference hallway meeting, a birthday party

• User shares contexts with contacts
  – policies not based on permissions or labels

• System infers all low-level details
  – in contrast to current practice...
App-centric Privacy: **Problematic**

- Permissions are abstruse
  - SD Card, File systems,...
  - 56 of 100+: dangerous
  - Statically assigned

- App owns user’s data
Data-centric Privacy: Problematic
Problem: User maps Contexts to Policies

Users

B’day Party

Class Project

Contexts

Apps

Files

Camera

Microphone

Wifi

System resources

System resources
Bubbles: Context-centric Security

- Data clusters around real-world contexts.
- Privacy policy as access control on contexts.
- Apps run in Bubbles; cannot affect privacy.
Using Bubbles

B’day Plans

email a caterer?

Time-line
Using Bubbles

B’day Catering

Time-line
Bubble is the Minimum Unit of Sharing

• Untrusted code can arbitrarily mix data inside a bubble.
  – Hence, sharing one item == sharing any item.

• Have to limit cross-bubble declassification
  – So that user has flexibility of re-sharing, e.g. meeting notes

• Bubbles have to be very light-weight contexts
  – I would put every 1:1 meeting at Usenix into a unique bubble
Challenges in implementing Bubbles

- Lots of bubbles → UI for navigating bubbles
- Apps don’t own data → API for developers
- System implementation → Infer dangerous permissions, and create light-weight containers
Local Bubbles

- Hike
- Sailing
- Wharf
- Tilden B’day Party
- Farmers Market
- Henry
Bubbles App Design Pattern

B’day Plan

Developer Zone
Updates, Ads, ...

B’day Party

Public profile info

User

Developer
Many Apps fit inside Bubbles

- Application-initiated sharing
  - Recommendation engines, Spam filters
  - Differential privacy, k-anonymity, ...

- User-initiated sharing
  - Storing, sharing, and editing docs
  - Real-time communication (voice, video)

- Anonymous: Not tied to real identity
  - Games, flashlights, wallpapers,
  - Browsing news, reviews, recipes, ...

<table>
<thead>
<tr>
<th>Percent</th>
<th>Free</th>
<th>Paid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>40%</td>
<td>60%</td>
</tr>
<tr>
<td>10</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>20</td>
<td>60%</td>
<td>40%</td>
</tr>
<tr>
<td>30</td>
<td>70%</td>
<td>30%</td>
</tr>
<tr>
<td>40</td>
<td>80%</td>
<td>20%</td>
</tr>
<tr>
<td>50</td>
<td>90%</td>
<td>10%</td>
</tr>
<tr>
<td>60</td>
<td>100%</td>
<td>0%</td>
</tr>
</tbody>
</table>
System Infers Dangerous Permissions

• User-controlled resources: 7
  – location, camera, microphone, read-contacts

• Virtualized resource: 27
  – internal and external storage, system logs, app cache and history,…

• Communication with firewall rules: 17
  – internet access, wifi, telephony
Context-centric Security

- Context = minimum unit of sharing data.
- Is working in contexts intuitive? Learnable?
- Does API support all useful functionality?
Backups.
Cloud-side Applications

- Cloud Storage
- Personal Documents
- Real-time applications
- E-commerce
- Social applications
- Miscellaneous: Browsing, peer-to-peer
Application-centric Security

HARDWARE CONTROLS
TAKE PICTURES AND VIDEOS
Allows the app to take pictures and videos with the camera.

NETWORK COMMUNICATION
FULL INTERNET ACCESS
Allows the app to create network sockets.

YOUR PERSONAL INFORMATION
READ CONTACT DATA
Allows the app to read all of the contact (address) data stored on your device and to send your data to other people.
WRITE CONTACT DATA
Allows the app to modify the contact (address) data stored on your device. Allows the app to modify or delete the contact data stored on your device.

Format QR CODE
Type ADDRESSBOOK
Time 6/1/11 2:55 PM
Metadata L

Homer Simpson
742 Evergreen Terrace
Springfield, USA
555-1234
hsimpson@snpp.com

Add contact  Show map  Dial number  Send email
Data-centric: Problematic

- Users: map privacy concerns to policies on labels?

```xml
<preventiveMechanism name="TaintPictures">
  <description>
    Adds taint 0x10000 for pictures taken at given location
  </description>
  <trigger action="uc.event.TAINTDROID">
    <paramMatch name="action" value="OSFileSystem.write" />
    <paramMatch name="taint" value="128" />
    <paramMatch name="location" value="49.445626;7.760339;50;true;false" />
  </trigger>
  <condition><true /></condition>
</authorizationAction>
```

```prolog
goal ProtectCallPrivacy(deny) :- L.connects(A,B) ∧ L.type(any) ∧ A.trustLevel(untrusted) ∧ ¬(A.hasPermission(INTERNET) ∧ (A.hasPermission(PHONE_STATE) ∨ A.hasPermission(PROCESS_OUTGOING_CALL))) ∧ B.trustLevel(untrusted) ∧ ¬(B.hasPermission(PHONE_STATE) ∨ B.hasPermission(PROCESS_OUTGOING_CALL)) ∧ B.hasPermission(INTERNET)
```
Data-centric: Labels and Policies

• Hard for the Users
  – Map privacy concerns to lattice of security labels

• Hard for benign Developers
  – How to write programs that work around labels?

```java
public static void main(String[] args) {
    String filename = args[0];
    final principal p = Runtime.user();
    final label lb;
    lb = new label(p);
    Runtime[p] runtime = Runtime.getRuntime(p);
}```
Bubbles App Design Pattern

- **B’day Party**
  - July 10

- **Developer Zone**
  - Calendar updates

- **Viewer**
  - Calendar layout

- **B’day Plan**
  - July 10

User

Developer
Bubble: The Minimum Unit of Sharing

• Navigating Bubbles

• Sharing data: user decides unit of sharing

• Light-weight contexts
  – User has flexibility of re-sharing, e.g. meeting notes
Context-centric Security

• Intuitive User interface

• Simple Developer API

• Efficient System