Addressing Data Reuse Issues at the Protocol Level

Oshani Seneviratne and Lalana Kagal
DIG, MIT CSAIL
June 8, 2011
Issues Addressed
#1: Personal Information on the Web

- Increasing amounts of personal information on the Social Web
- Often times there are unforeseen adverse consequences
- Users become victims of poor design choices: *E.g.* Facebook Beacon, Google Buzz, etc
#1: Personal Information on the Web

- Users do not understand how to use privacy controls effectively: E.g: Google Latitude

- Web is an easy medium to copy and paste

- How can we make sure that these information misuses do not happen?
#2: Reuse of Creative Works

• There’s so much content on the Web
  – 3.6 billion images on flickr
  – 20 hours of video uploaded every minute on YouTube

• Content reuse is good
  – Prevents redundant work
  – Promotes creativity
#2: Reuse of Creative Works

• But even with these mechanisms, content misuse is pretty common

• How can you prove that someone has violated your usage restrictions?
Proposed Solution

HTTPA

Accountable Hyper Text Transfer Protocol
Accountability to Supplement Access and Usage Control
Intention
"I will only use the data for educational purposes"
Usage Restriction Specification

• Initial Implementation of the protocol will use the RMP (Respect My Privacy) ontology

• Usage Restriction needs terms such as:
  
  – No tracking
  – No ownership transfer
  – No commercial use
  – No depiction
  – No employment use
  – No insurance use
Negotiation of Usage Restrictions and Intentions / Handshake

- Uses HTTP headers ‘usage-restrictions’ and ‘intentions’

- Use ‘negotiate’ when the original usage restrictions and intentions do not match
Data Uploaded to Websites (I)

POST picture
Usage Restrictions: No Ownership Transfer

HTTPA 412 Precondition Failed
Intentions: Ownership Transfer

POST picture
Negotiate: No Ownership Transfer

HTTPA 204 No Content
Data Uploaded to Websites (II)

POST picture
Usage Restrictions: No Ownership Transfer

HTTPA 412 Precondition Failed
Intentions: Ownership Transfer

POST picture

myspace
facebook
orkut
Data Downloaded from Websites

GET Alice’s Photo
Intentions: No-Commercial

Usage Restrictions: No Ownership Transfer

GET Alice’s Photo
Intentions: No-Commercial, No Ownership Transfer

HTTPA 200 OK
Usage Aware Log: Log URI
Conclusions

• **Policy enforcement** is not enough to solve security and privacy problems on the web.

• We need a **web ecosystem** supporting **accountability** to supplement policy enforcement.
WE'RE IN A NARROW WINDOW IN WHICH PEOPLE ARE USING GOOGLE LATITUDE, BUT HAVEN'T LEARNED THE HABIT OF TURNING IT OFF WHEN THEY'RE DOING SOMETHING DISCREETLY.

I WROTE AN APP TO LOG FRIENDS' LOCATIONS AND WORK OUT ADDRESSES AND BUSINESS NAMES.

<table>
<thead>
<tr>
<th>TIME</th>
<th>MEGAN</th>
<th>ROBERT</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00 AM</td>
<td>HOME</td>
<td>HOME</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>EASTVIEW ADULT TOY STORE</td>
<td>HOME</td>
</tr>
<tr>
<td>1:30 PM</td>
<td>HOME</td>
<td>SCHOOL</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>LAKETOWN SEX TOY SHOP</td>
<td></td>
</tr>
<tr>
<td>2:30 PM</td>
<td>HOME</td>
<td></td>
</tr>
<tr>
<td>3:00 PM</td>
<td>FRY'S ELECTRONICS</td>
<td></td>
</tr>
<tr>
<td>3:30 PM</td>
<td>ED'S POWER TOOL EMPORIUM</td>
<td>SUBWAY</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>HOME</td>
<td></td>
</tr>
<tr>
<td>4:10 PM</td>
<td>HOSPITAL BURN WARD</td>
<td></td>
</tr>
</tbody>
</table>

Source: http://xkcd.com/596/
Questions?
oshani@mit.edu