Privacy-Preserving Social Plug-ins

Georgios Kontaxis‡, Michalis Polychronakis‡, Angelos D. Keromytis‡, and Evangelos P. Markatos*

‡Columbia University and *FORTH-ICS
What is this talk about?

• Social plug-ins today pose a serious privacy risk that most users don’t know about

• Privacy risk remains even if one doesn’t use social plug-ins

• We propose and implement a novel design for privacy-preserving social plug-ins without sacrifices in functionality

• Our design could be adopted by social networks as service
What are Social Plug-ins?

- Provided by online social networking services (SNS)
- Included in third-party Web sites
- Enable users to interact with the page content through their social identity via a series of actions:
  - Offer personalized information based on social data

![Social Plugin Icons]

- Like
- +1
- Recommend
- Send
- Share
- Tweet
- Follow
How popular are Social Plug-ins?

- Facebook has 955 million users (Facebook Newsroom 2012)
- 33% of the Top 10K Web sites have integrated the Like button (at least 2 million in total)
- Google Mail has 425 million users (Google I/O 2012)
- 22% of the Top 10K Web sites have integrated the +1 button (at least 1 million in total)
How do Social Plug-ins Work?

1. Page Content
2. Request
3. Personalized Content

Non-personalized

Personalized

John Doe, Jane Doe and 69 others like this.
Privacy Risks of Social Plug-ins

- The ubiquity of social plug-ins enables cross-site tracking
  - 23% of the sites have a FB plug-in
    [Roesner et al. NSDI 2012]
- Social networking services know the user’s real name
  (vs advertisement networks)
- Don’t have to interact with a plug-in
- Cannot know beforehand whether a page carries social plug-ins
Who knows I visited wired.com?
Preventing Privacy Leaks

• Logging Out of the Social Networking Service?
  – In 2011 at least 3 FB cookies persisted after logout
    One of them was the user’s unique ID!
    • Facebook classified this as a bug and fixed it
  – Today (2012) at least 2 cookies persist 😊
    • uniquely identify “public computers”, “suspicious activity”

(a) 43 likes. Sign Up to see what your friends like.
(b) 43 people like this.
(c) Jane Doe, John Doe and 41 others like this.

Never logged in Facebook
Logged in, then logged out
While logged in
Preventing Privacy Leaks

• Disabling Third-party Cookies?
  – Social plug-ins will render as if the user is not a member of the social networking service
  – However, doesn’t always protect from third-party tracking

<table>
<thead>
<tr>
<th></th>
<th>[R]</th>
<th>[W]</th>
<th>[R]</th>
<th>[W]</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.E. 9</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Firefox 13</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Chrome 21</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

• In Chrome it’s trivial for a third party to position itself as a first party (popup window – native blocker won’t help)
• In Safari third party cookies are blocked unless the user interacts with them (or an automated script submits an HTML form)
Preventing Privacy Leaks

• Enabling the Do Not Track HTTP Header?
  – Signal “opt-out from tracking” to the receiving Web site
  – Policy technique, no technical enforcement
  – The definition of tracking is still up for discussion
  – Very few sites support it at the moment

• Removing third parties from Web pages?
  – Commonly used to filter out advertisements
  – Social plug-ins will not appear in the page at all
  – Users lose the option of viewing and/or interacting with some of the social plug-ins if they want to
Privacy vs Functionality Dilemma

• Users are asked to choose between:
  – Privacy but also loss of personalization or social plug-ins altogether
    OR
  – Functionality but also sharing Web activity with social networks

• Why should there be a dilemma? 😊
Privacy-Preserving Social Plug-ins
The SafeButton Browser Extension

- For Chrome and Firefox
- Disables the original social plug-ins
- SafeButton DOM replacements preserve the same (personalized) content
- Upon interaction, the original plug-in is loaded to enable write functionality
# SafeButton’s Social Plug-in Support

<table>
<thead>
<tr>
<th>Provider</th>
<th>Social Plug-in</th>
<th>SafeButton Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>Like</td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>Send</td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>Comments</td>
<td>Partial*</td>
</tr>
<tr>
<td>Twitter</td>
<td>Tweet</td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>Follow</td>
<td>Complete</td>
</tr>
<tr>
<td>Google Plus</td>
<td>+1</td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>Share</td>
<td>Complete</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>Recommend</td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>Shared</td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>Follow</td>
<td>Complete</td>
</tr>
</tbody>
</table>

*API shortcomings*
SafeButton’s Bootstrapping

– Privacy protected from the beginning

– Downloading social data upon user’s login to social network service

– Bootstrapping the local store for 5,000 friends took a little less than 10 hours (room for optimization)

– Periodic, incremental updates
SafeButton’s Resource Requirements

11.3MB for a user with 400 friends (avg. friend count in dataset)

5.4MB for a user with 190 friends (avg. friend count on Facebook)
SafeButton’s Performance

![Bar chart showing the performance of SafeButton, including X-Cache hit and miss, and comparing to Original Social Plugin.](image)

- **SafeButton X-Cache hit**
- **SafeButton X-Cache miss**
- **Original Social Plugin**

Legend:
- □ Processing
- ■ Network: request dispatch to first response byte
- ◼ Network: first response byte to end of transmission
- ▲ DataStore lookup

*Time in milliseconds*
SafeButton As a Service

• Web browser extensions are not good enough
  – Users unaware of privacy risks of social plug-ins
  – Users unwilling or unable to install extensions
  – Adoption of AdBlock 3.1%, NoScript 0.4% in Firefox

• Ideally we want a design offered by social networking services themselves

• Implemented with Web technologies that enable an in-browser solution without additional software
SafeButton As a Service

- Pages incl. social plug-ins as usual
- Social network will return a SafeButton agent

How to avoid leaking user-identifying information in the process?
- Isolate social plugins to diff. domain
- Secure message passing with SNS
- Fragment identifiers parameters
- Cachable agent
- Encrypted data store
Discussion

• Keeping social data locally in the client may introduce security risks (malware, snooping friends, stolen disk)
  – Is it really that different from keeping the data in the cloud but running untrusted software in the user’s computer?
  – It’s equally easy for tech-savvy friends to install key-logging software or inspect SafeButton’s data store
  – An encrypted SafeButton data store will provide the same protection against disk theft as will the user’s practice of logging out (or not) from social networking services.
Summary

• Identified privacy issues of current social plug-ins that most users aren’t aware of
• Pointed out the dilemma between privacy and functionality
• Presented our proposal for privacy-preserving social plug-ins which eliminates that dilemma
• Suggested a novel design for privacy-preserving social plug-ins as a service

http://tinyurl.com/safebutton

kontaxis@cs.columbia.edu