Privacy-Preserving Social Plugins

Evangelos Markatos
FORTH-ICS, Crete Greece
in collaboration with

G. Kontaxis, M. Polychronakis and A. Keromytis
Columbia University

Work appears in USENIX SECURITY 2012
Outline

- What is the problem?
  - Erosion of privacy on the Internet
  - How do social networks contribute to it?
- Are there any solutions?
- What do we propose?
  - SafeButton
Outline

- What is the problem?
  - Erosion of privacy on the Internet
  - How do social networks contribute to it?
- Are there any solutions?
- What do we propose?
  - SafeButton
We live in times of change

- Social Networks have changed their model
  - They used to be the place to
    - Hang out with friends
    - Catch up with news
    - Play an occasional game
    - Something like a virtual “café”
  
- Their new model:
  - To become the single
    - Authentication and personalization service on the web
    - Via “social plugins”
This is what I “like”

10 April 2012, Bern, Switzerland

EUROSEC
2012 European Workshop on System Security

Workshop Registration Information

Registration to EuroSec 2012 is handled through the EuroSys online registration system. Keep in mind that there are some usability issues with the registration system when registering using the Safari/Chrome browsers.

All registration fees are payable in Swiss Francs (CHF). General conditions and the exact rates that apply are detailed in the EuroSys 2012 Registration Information page. For any questions regarding the registration, please contact the EuroSys 2012 Finance Chair.
More of what I “like”
The problem

- In order for FB to personalize a web page
  - It needs to know that I have visited the web page
- FB knows all the “like-enabled” web pages I visit
  - All the news that I read
  - All the videos I see
  - All the medical info I search for
  - Political sites? Religious sites?
  - - even if I do not “like” them

Privacy?
What is the extent of the problem?

- 20% of the top 10K Web sites include the “like” button
- Data from [http://trends.builtwith.com/widgets/Facebook-Like](http://trends.builtwith.com/widgets/Facebook-Like)
So

- 1 out of 5 web sites
  - Will tell FB when you visit the site
- Do you know which web sites will tell?
  - No
- Can you ask the web site not to tell?
  - No
- Is there any way to protect yourself?
  - maybe...
Outline

- What is the problem?
  - Erosion of privacy on the Internet
  - How do social networks contribute to it?
- Are there any solutions?
- What do we propose?
  - SafeButton
What can I do?

- Use an Anonymizing service such as TOR
  - Good, but it is just like accessing FB from TOR
    - It hides my IP address, but
    - I use my real name and password to log into FB
What can I do?

- **Log out** from Social Networks
  - Not always possible/convenient
    - If I log out of Google+ I am out of Gmail
    - If I use Gmail I am on Google+ automatically as well
      - Single-sign on approach
  - Sometimes it is not even enough:
What can I do?

- Use a **Cookie Blocker**
  - plug in which strips cookies
- Do not send the Social Network cookie
  - Yes, but I will not have any personalization
    - I want to know what my friends like
    - I want to know how many of my friends like this page
    - I want to see their recommendations
So...

- The seems to be a dilemma here:
  - Privacy advocates suggest that
    - Privacy is important
      - Forget personalization use cookie blockers
  - Social Networks suggest that
    - Personalization is the next best thing
      - OK to sacrifice a little privacy

- We say:
  - This is a **false dilemma**
    - You can have both!
Outline

- What is the problem?
  - Erosion of privacy on the Internet
- Are there any solutions?
- What do we propose?
  - SafeButton
Our approach: Safe Button

- We propose: SafeButton
  - Prevent the browser
    - from contacting the source of a social plugin
  - Create a local store (i.e. a cache) of
    - Social information
    - About the user and her friends
  - Use the local cache to personalize web pages
  - Populate the cache off-line
The code:

```plaintext
GET /plugins/like.php?app_id=APP_ID&href=TARGET_URL&send=false&layout=box_count&width=90&show_faces=false&action=like&colorscheme=light&font&height=62 HTTP/1.1

Host: www.facebook.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.2 (KHTML, like Gecko) Chrome/15.0.874.106 Safari/535.2
Accept: text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8
Referer: EMBEDDING_PAGE_URL
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US, en; q=0.8, el; q=0.6
Accept-Charset: ISO-8859-1, utf-8; q=0.7, *; q=0.3
Cookie: datr=DATR; c_user=CURRENT_USER; xs=SESSION_ID
```

Listing 1. HTTP GET request for loading a Facebook Like button.
How does this work?
SafeButton

- Populating the local store with information.
- Social networks expose a developer’s API.
  - Fetched information is data the user already has access to via his/her online profile.
- Instead of asking
  - (1) “has Bob liked page A?”
    - we ask
  - (2) “gimme all the likes Bob has ever made”.
    - and we store it
    - and we are able to perform query (1) offline
    - And the SN does not know that Bob visited page A 😊
The data flow

**Before**

- Third-party Website
- Social Network
  - Page Content
  - Request
  - Personalized Content
  - Social Plugin

**After**

- Third-party Website
  - Page Content
  - Personalized Content
  - Social Plugin
  - Non-authenticated Request
  - Public Data
  - Local DataStore
  - Private Data

site: www.example.com
cookie: user-ID
Is it practical?

- Average user (190 friends) needs just 5.4MB of storage.
- Extreme case (5,000 friends) requires a reasonable (even for mobile devices) amount of space (145.7MB).

<table>
<thead>
<tr>
<th>Data</th>
<th>190 Friends</th>
<th>5,000 Friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names, IDs of Friends</td>
<td>10.5KB</td>
<td>204.8KB</td>
</tr>
<tr>
<td>Photos of Friends</td>
<td>463.4KB</td>
<td>11.8MB</td>
</tr>
<tr>
<td>Likes of Friends</td>
<td>4.6MB</td>
<td>126.7MB</td>
</tr>
<tr>
<td>Shares of Friends</td>
<td>318.4KB</td>
<td>7.0MB</td>
</tr>
<tr>
<td>Total</td>
<td>5.4MB</td>
<td>145.7MB</td>
</tr>
<tr>
<td>Average (per friend)</td>
<td>29.2KB</td>
<td>29.7KB</td>
</tr>
</tbody>
</table>
It’s also fast!

- Safebutton downloads only raw data contrary to what the Facebook plugins are doing right now. *(x2.8 faster)*
- Caching frequently used data locally enables almost instantaneous plugin rendering. *(x14.6 faster)*
Summary

- Social Networks change their business model
  - To be come the single personalization and authentication service on the Internet
- Erosion of privacy
- Social Networks know 20%
  - of the popular web sites we visit
- Traditional anonymization does not help
- We propose SafeButton
Privacy-Preserving Social Plugins

Evangelos Markatos
FORTH-ICS, Crete Greece
in collaboration with
G. Kontaxis, M. Polychronakis and A. Keromytis
Columbia University

Work appears in USENIX SECURITY 2012
SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet

Evangelos Markatos
FORTH-ICS
Outline of the talk

- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger
- What are we doing about this?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet
Outline of the talk

- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger

- What will we do?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet
Government: UK Parliament’s PCs infected

The Houses of Parliament IT system has become infected with the Conficker computer virus, it has emerged, raising questions about possible security flaws at the Palace of Westminster.
Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen  March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin’s High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership’s four Austin area lots.
Energy: No electricity

Energy Resources

Computer virus in Australian power grid

Published: Oct. 2, 2009 at 4:22 PM

SYDNEY, Oct. 2 (UPI) -- A “sinister” computer virus has infected computers controlling Australia’s Integral Energy power grid.
Defense: fighter planes grounded

French fighter planes grounded by computer virus

French fighter planes were unable to take off after military computers were infected by a computer virus, an intelligence magazine claims.

by Kim Willsher in Paris
Published: 11:43AM GMT 07 Feb 2009
Last but not least: Stuxnet!

Tailored specifically against SCADA systems, is the most recent demonstration that not only attacks are sophisticated, complex and well-coordinated. It also demonstrates that the bad guys:

- are very well-equipped
- have ambitious goals (cyber-physical systems)
Rent-a-botnet!

The Day Before Zero
An Ongoing Conversation About Targeted Attacks

Want to rent an 80-120k DDoS Botnet?

Over recent weeks there has been a lot of interest in DDoS botnets – that is to say, rentable botnets that provide DDoS as a managed service. I’ve spoken to a number of people about how easy this is to do, and how practically anyone who happens to know how to use a popular Internet search engine can probably locate the sellers or the hacking message boards they hang around. Perhaps one of the finer points missing about the discussion of renting DDoS botnets pertains to the size.

A fairly typical rate for DDoS botnet rental hovers around the $200 for 10,000 bot agents per day. The rate per day is fairly flexible, and influenced by the actual size of the botnet that the bot master is trying to section off for DDoS services.

There is even a free 3-minute trial!
Outline of the talk

- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger

- What will we do?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet
Predicting “what’s next”

- **SysSec**: managing threats and vulnerabilities for the future Internet
  - a NoE, 2010-2014
  - General approach
    - **Proactive solutions**
    - **Collaborate**
      - At a European level
      - With our international colleagues

- Politecnico di Milano (IT)
- Vrije Universiteit (NL)
- Institute Eurecom (FR)
- BAS (Bulgaria)
- TU Vienna (Austria)
- Chalmers U (Sweden)
- TUBITAK (Turkey)
- FORTH – ICS (Greece)
SysSec proposes a *game-changing* approach to cybersecurity:

- Currently Researchers are mostly *reactive*:
  - they usually track cyberattackers *after* an attack has been launched
  - thus, researchers are always one step behind attackers

- SysSec aims to break this vicious cycle

- Researchers should become more *proactive*:
  - **Anticipate** attacks and vulnerabilities
  - **Predict** and prepare for future threats
  - Work on defenses *before* attacks materialize.
1. Create an active, vibrant, and collaborating **community of Researchers** with
   - the expertise, capacity, and determination to *anticipate* and mitigate the *emerging* threats and vulnerabilities on the Future Internet.
   - SysSec aims
     - to create a *sense of “community”* among researchers,
     - to *mobilize* this community,
     - to *consolidate* its efforts,
     - to *expand their collaboration* internationally, and
     - become the *single point of reference* for system security research in Europe.
2. Advance European Security Research well **beyond** the state of the art
   - research efforts are **fragmented**
   - SysSec aims to **provide a research agenda** and
   - **align their research activities** with the agenda
   - make SysSec **a leading player** in the international arena.
3. **Create a virtual distributed Center of Excellence** in the area of emerging threats and vulnerabilities.
   - By forming a **critical mass** of European Researchers and by aligning their activities,
   - A **leading role internationally**, empowered to undertake **large-scale**, ambitious and high-impact research efforts.

4. **Create a Center of Academic Excellence** in the area
   - create an education and training program targeting young researchers and the industry.
   - lay the **foundations** for a common graduate degree in the area with emphasis on Systems Security.
5. Maximize the impact of the project by proactive dissemination to the appropriate stakeholders.
   - disseminate its results to international stakeholders so as to form the needed strategic partnerships (with similar projects and organizations overseas) to play a major role in the area.
   - dissemination within the Member States will
     - reinforce SysSec's role as a center of excellence and
     - make SysSec a beacon for a new generation of European Researchers.

6. Create Partnerships and transfer technology to the European Security Industry.
   - create a close partnership with Security Industry
   - facilitate technology transfer wherever possible to further strengthen the European Market.
**1st SysSec Workshop**

- **By the numbers:**
  - 23 position papers
    - i.e. where is the security research going?
  - 6 (longer) Student/Research papers
  - 95 authors
  - 36 organizations
  - One session on INCO strategy
    - In trustworthy ICT
    - Organized by the BIC project
1st SysSec Workshop – Who?
Research Roadmap

cyberattacks
mobile
SCADA vulnerabilities
online fraud
research
attacks to the cloud
botnets
drive-by downloads
social networks
DDoS malware
mobile malware
mobile rootkits
phishing
identity theft
underground economy
mobile piracy
mobility
scareware
trojans
memory corruption
privacy
How to collaborate with SysSec?

- Join our constituency (mailing list):
  - http://www.syssec-project.eu

- Contribute to the research roadmap
  - Read it at http://t.co/ZbiM0cpl
  - Provide feedback on emerging threats

- Contribute to our systems security University curriculum
  - Contribute homeworks/exams, lab exercises
  - Teach some of the courses at your University

- Send your students to the partners
  - with SysSec Scholarships

- Send your graduates to the SysSec partners
  - With SysSec Marie Curie Fellowships

- Participate in the SysSec Summer School
  - Fall 2012 Amsterdam
Summary

- Hackers are getting more sophisticated
- The impact of cyberattacks is getting higher
- We need to collaborate to manage emerging threats on the future Internet
  - SysSec started on Sept 1\textsuperscript{st} 2010.
  - Help us define future security threats
  - Help us teach our students system security
  - Join us to break the vicious cycle of cyberattacks.
SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet

http://www.syssec-project.eu
http://twitter.com/syssecproject

Evangelos Markatos
FORTH-ICS
Fallback Slides
The internals: Why is there a privacy leak?

- Plugins embedded as iFrames in third-party Web pages.
- Web Browser transmits to the online social network, whether the user interacts with the plugin or not:
  - URL of embedding page
  - User’s unique identifier (cookie) for that social network.
  - User may be carrying such identifier even if logged out.
Why is this a problem?

- The erosion of privacy on the Web
- We are going to describe how social plugins (such as the “like” Button) contribute to the erosion of people’s privacy