

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

Overview

Organisation

Spread the word

Programme

Registration

Submit a paper

Workshop Registration Information

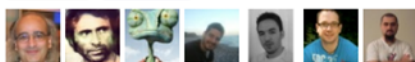
Registration to EuroSec 2012 is handled through the [EuroSys online registration system](#). Keep in mind that there are some usability issues with the registration system when registering using the Safari/Chrome browsers.

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.



+10 Recommend this on Google

Like Send Evangelos Markatos, Manolis Stamatogiannakis and 19 others like this.



All pages © 2011-2012 [EUROSEC12 Organization Committee](#). Hosting & support kindly provided by [syssec](#).

More of what I “like”



9th Conference on
Detection of Intrusions and Malware & Vulnerability Assessment

July 26-27th, 2012
Heraklion, Crete, Greece

[Welcome](#) — [Calls](#) — [Guidelines](#) — [Committees](#) — [Local Information](#) — [Registration](#) — [Submit](#)

welcome

The annual DIMVA conference serves as a premier forum for advancing the state of the art in intrusion detection, malware detection, and vulnerability assessment. Each year, DIMVA brings together international experts from academia, industry, and government to present and discuss novel research in these areas. DIMVA is organized by the special interest group [Security – Intrusion Detection and Response \(SIDAR\)](#) of the [German Informatics Society \(GI\)](#). The conference proceedings will appear in Springer's [Lecture Notes in Computer Science \(LNCS\)](#) series.

important dates

Paper submission deadline

2 March 2012 23:59 EST

24 Feb 2012 23:59 EST

Paper acceptance notification

13 Apr 2012

Camera-ready deadline

30 Apr 2012



+2 Recommend this on Google



Send

Manolis Stamatogiannakis, Georgios Chinis and 4 others like this.

twitter news feed

- about 24 days ago we said, Have you booked your hotel for #DIMVA 2012? Check the suggested hotels on the conference website: <http://t.co/tGnjPU7q>
- about 44 days ago we said, Accommodation information for #DIMVA 2012: <http://t.co/tGnjPU7q>
- about 85 days ago we said, Still preparing your #DIMVA paper? Remember that a last-minute update is quicker than a last-minute submission. Submit your paper now!



All our tweets.


The problem

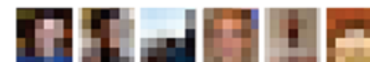
- In order for FB to personalize a web page
 - It needs to know that I have visited the web page
- FB knows all the “like-enabled” web pages I visit
 - All the news that I read
 - All the videos I see
 - All the medical info I search for
 - Political sites? Religious sites?
 - - even if I do not “like”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

Privacy?

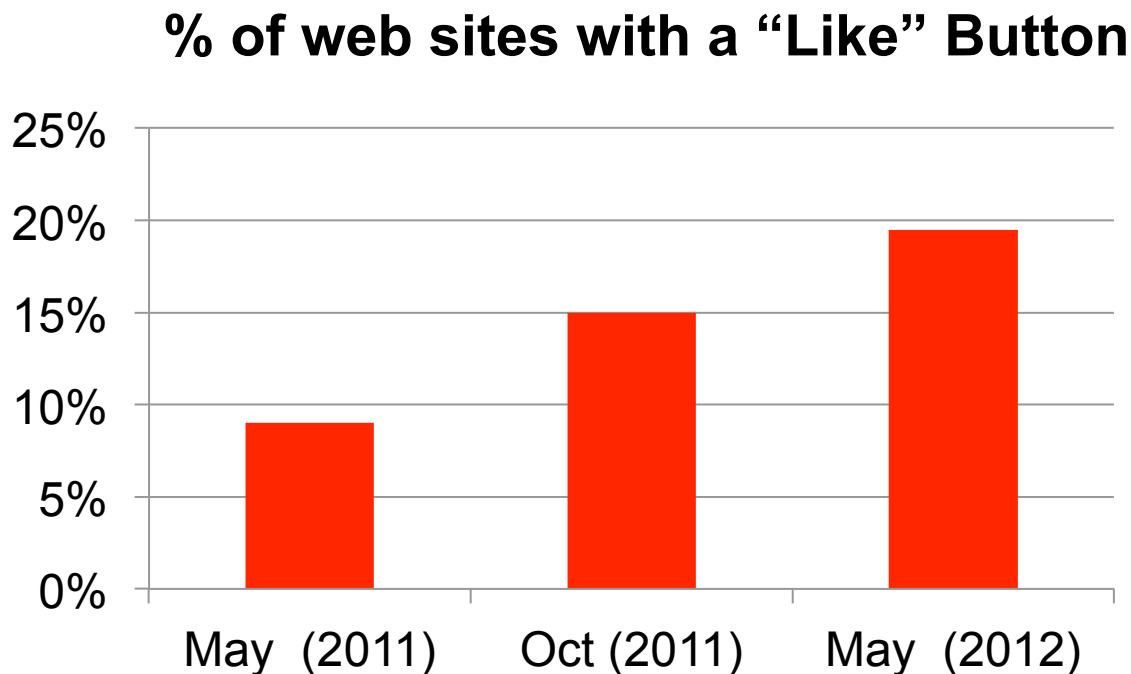
(a)  43 likes. Sign Up to see what your friends like.

(b)  43 people like this.

(c)  Jane Doe, John Doe and 41 others like this.



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>

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:
 - <http://nikcub.appspot.com/posts/logging-out-of-facebook-is-not-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

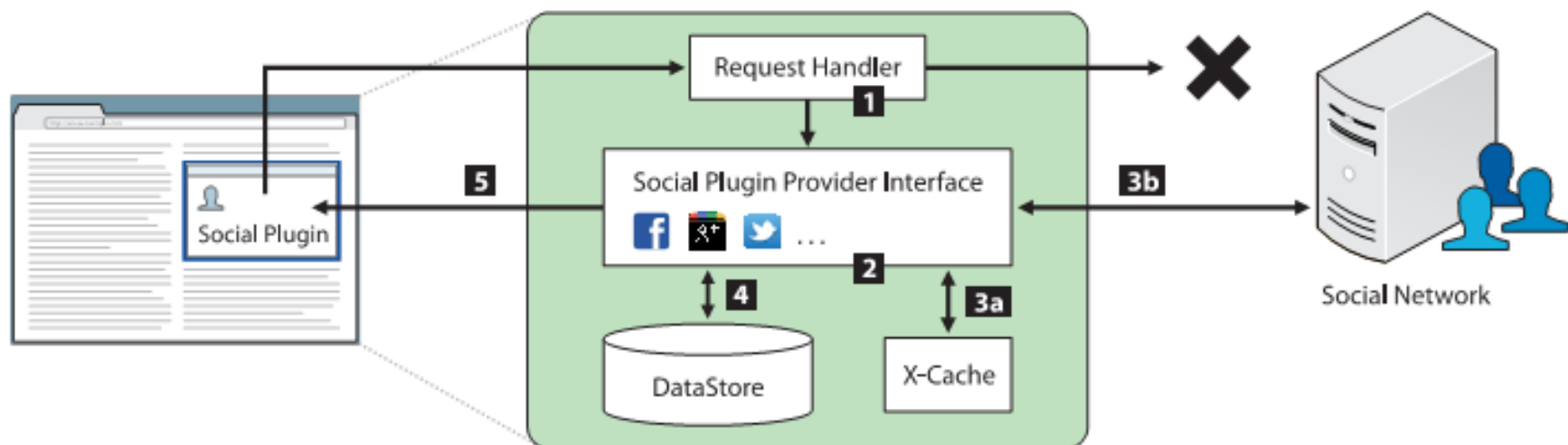
- We propose: SafeButton
 - Prevent the browser
 - from contacting the source of a social plugin
 - Create a **local store (i.e. a cache)** of
 - Social information
 - About the user and her friends
 - Use the local cache to personalize web pages
 - Populate the cache off-line

The code:

```
1 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
2 Host: www.facebook.com
3 Connection: keep-alive
4 User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit
   /535.2 (KHTML, like Gecko) Chrome/15.0.874.106
   Safari/535.2
5 Accept: text/html,application/xhtml+xml,application/xml;
   q=0.9,*/*;q=0.8
6 Referer: EMBEDDING_PAGE_URL
7 Accept-Encoding: gzip, deflate, sdch
8 Accept-Language: en-US,en;q=0.8,el;q=0.6
9 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
10 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?

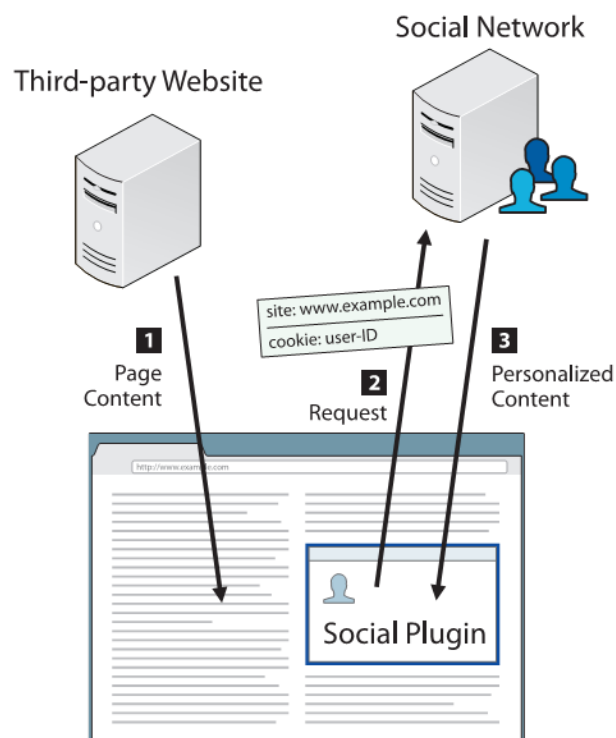


SafeButton

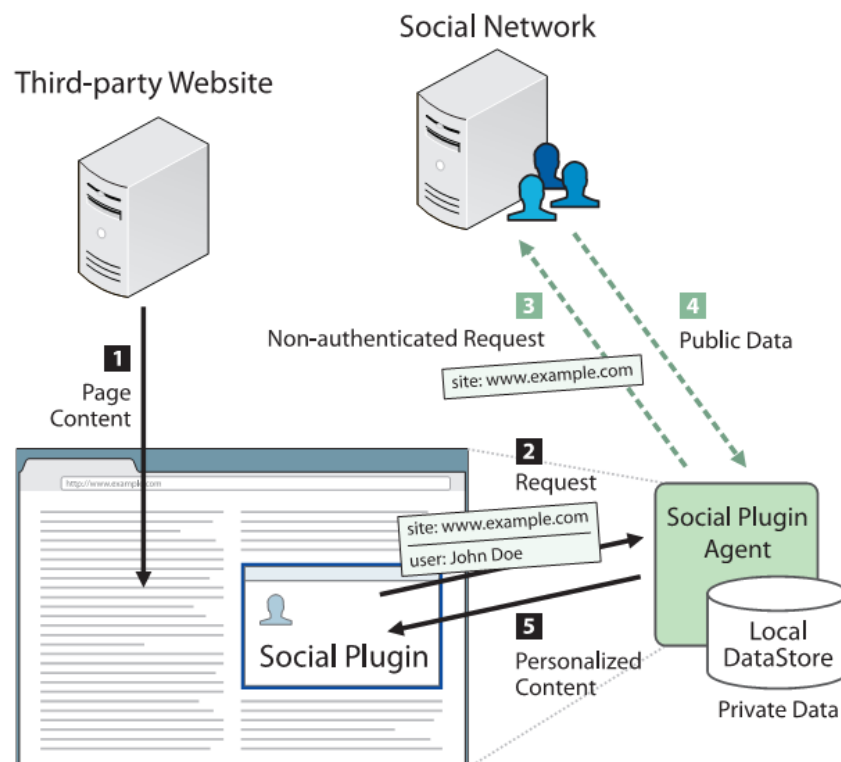
- Populating the local store with information.
- Social networks expose a developer's API.
 - Fetched information is data the user already has access to via his/her online profile.
- Instead of asking
 - (1) “has Bob liked page A?”
we ask
 - (2) “gimme all the likes Bob has ever made”.
 - and we store 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



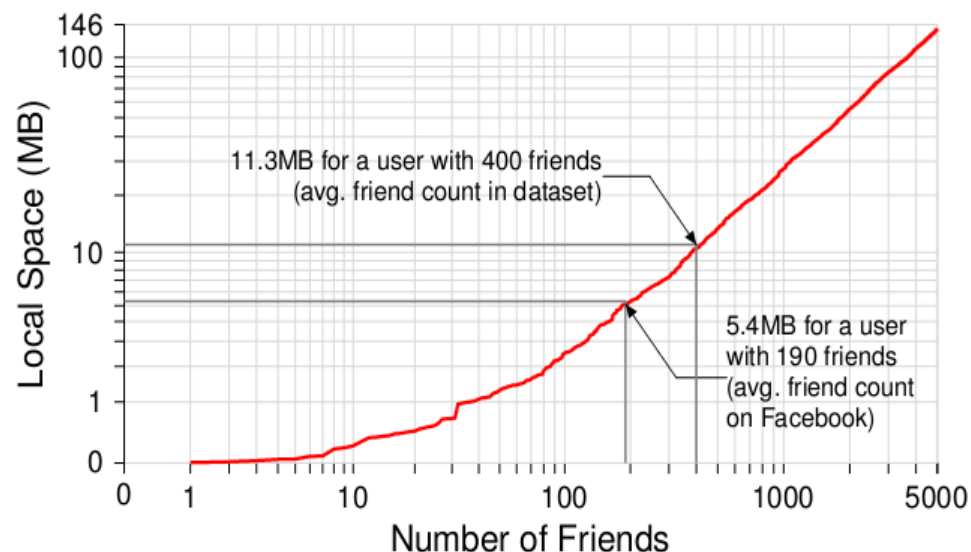
After



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).

Data	190 Friends	5,000 Friends
Names, IDs of Friends	10.5KB	204.8KB
Photos of Friends	463.4KB	11.8MB
Likes of Friends	4.6MB	126.7MB
Shares of Friends	318.4KB	7.0MB
Total	5.4MB	145.7MB
Average (per friend)	29.2KB	29.7KB



Speed

- 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*)

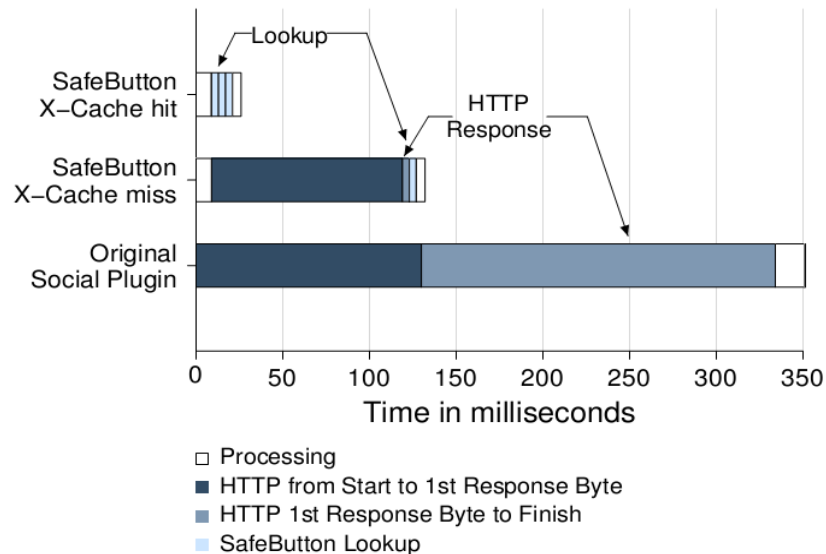


Fig. 7. Detailed timeline of the events taking place to load and fully render render a Like button with and without SafeButton.

Summary

- Social Networks change their business model
 - To become 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



[Home](#)
[News](#)
[Election 2010](#)
[Sport](#)
[Finance](#)
[Lifestyle](#)
[Comment](#)
[Travel](#)
[Culture](#)
[Fashion](#)
[Jobs](#)
[Dating](#)
[Subscriber](#)
[Offers](#)

[Technology](#)
[Motoring](#)
[Health](#)
[Property](#)
[Gardening](#)
[Food and Drink](#)
[Family](#)
[Outdoors](#)
[Active](#)
[Relationships](#)
[Expat](#)

[Technology News](#)
[Reviews](#)
[Topics](#)
[Advice](#)
[Video Games](#)
[Blogs](#)
[Video](#)
[Technology Debate2010](#)

HOME > TECHNOLOGY > MICROSOFT

Houses of Parliament computers infected with Conficker virus

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.

By Matthew Moore
Published: 7:00AM GMT 27 Mar 2009



The Conficker virus has infected computers in the Houses of Parliament Photo: GETTY

[Share](#)
[f](#)
[v](#)

Digg
0

[Email](#)
[Print](#)

Text Size

[Microsoft](#)
[News](#)
[Politics](#)
[UK News](#)

[Ads by Google](#)

[Anti Virus](#)
[Computer Virus Clean](#)

TECHNOLOGY TOPICS

- Microsoft in depth
- Technology picture galleries
- Apple in depth
- Google in depth
- Sony in depth
- Nintendo in depth

TELEGRAPH.CO.UK ON DIGG

[Popular Today](#)
[Upcoming](#)
[Related](#)

271 Drug-free inmates put on methadone before they are released

494 Scientists find new species of lizard with double penis

306 Ring of fire: Annular solar eclipse in Asia and Africa [PIC]

329 Rocking the Taliban

304 Viewers think new Doctor Who is 'too sexy'

255 Stressed teachers 'considering suicide'

content by **Telegraph.co.uk** powered by **digg**

Transportation: Cars out of control

WIRED[SUBSCRIBE >>](#)[SECTIONS >>](#)[BLOGS >>](#)[REVIEWS >>](#)[VIDEO >>](#)[HOW-TOS >>](#)[Sign In](#) | [RSS Feeds](#)

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE



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



[Done](#)

Energy: No electricity

[Mobile UPI](#) | [About UPI](#) | [UPI en Español](#) | [UPIU - University Media Alliance](#) | [My Account](#)

Search:

[Home](#) | [Top News](#) | [Entertainment](#) | [Odd News](#) | [Business](#) | [Sports](#) | [Science](#) | [Health](#) | [Real Estate](#) | [Photos](#) | [Videos](#)

[Resource Wars](#) [Global Water Issues](#)

You are here: [Home](#) / [Energy Resources](#) / [Computer virus in Australian power grid](#)

Energy Resources

[View archive](#) | [RSS Feed](#) [Receive Free UPI Newsletter](#)

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

www.proinso.net [Ads by Google](#)

Defense: fighter planes grounded

Telegraph.co.uk

Home News Election 2010 Sport Finance Lifestyle Comment Travel Culture F
UK World Celebrities Obituaries Weird Earth Science Health News Education Topics Ne
USA Barack Obama Europe Asia China Middle East Africa and Indian Ocean Australi

HOME NEWS WORLD NEWS EUROPE FRANCE

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



Share | f | |

663 diggs digg it

0 tweet

Email | Print

Text Size + -

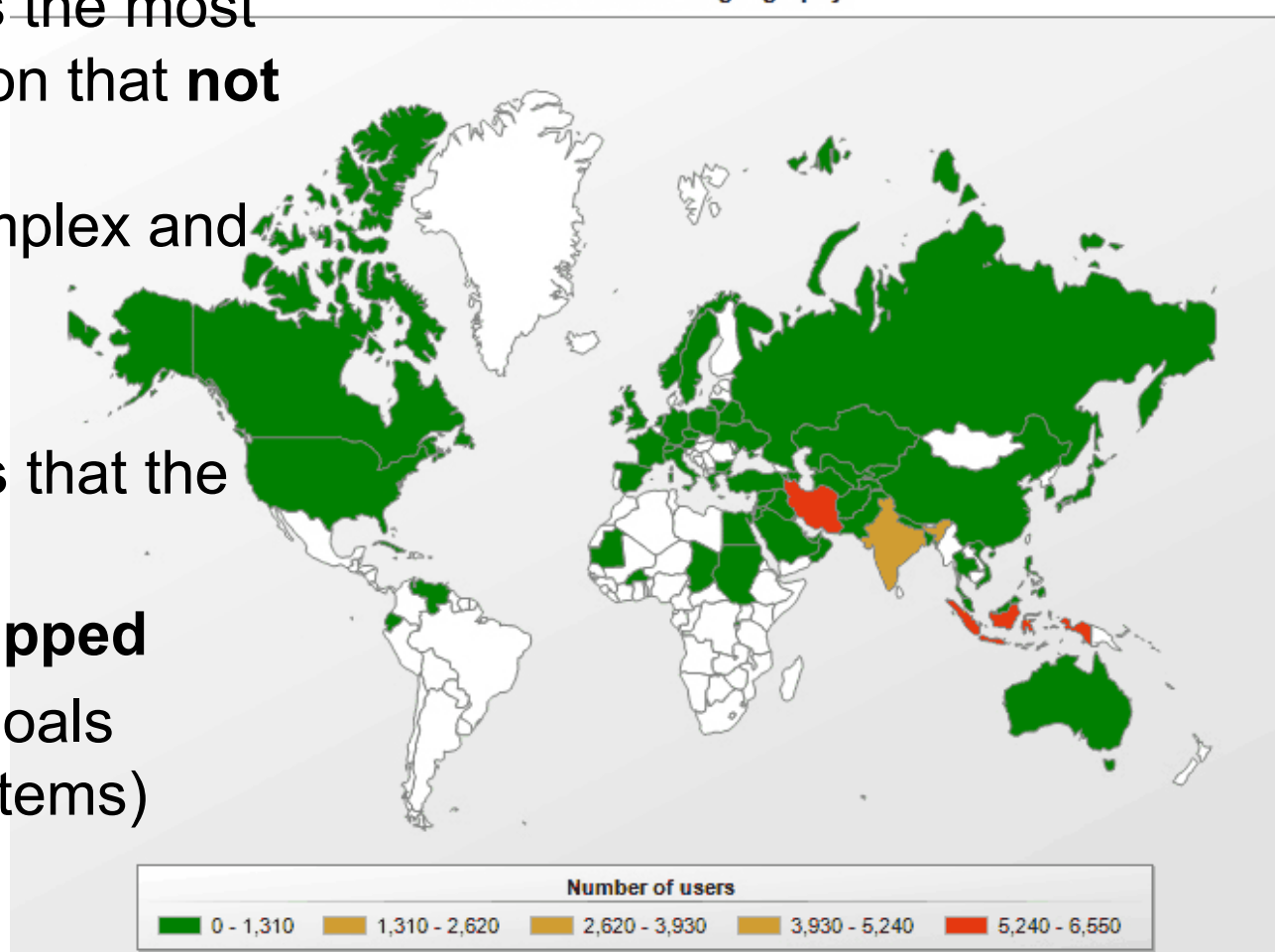
Last but not least: Stuxnet!

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)

Rootkit.Win32.Stuxnet geography



Rent-a-botnet!



The Day Before Zero

An Ongoing Conversation About Targeted Attacks

« Sizing a botnet – “You’re doing it wrong!”

ISP’s Dealing with Botnets »

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

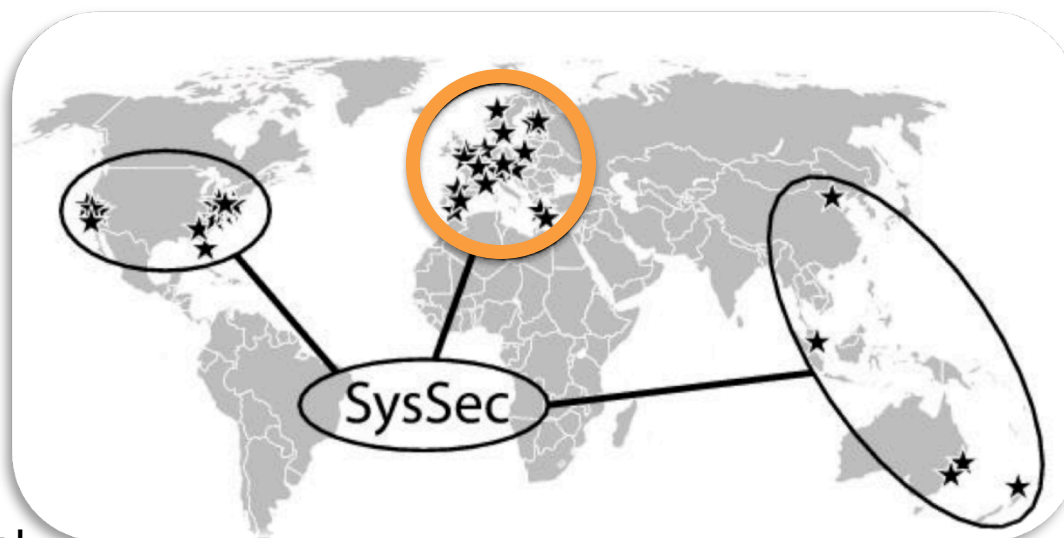
- Security Challenges: What is the problem?
 - Hackers are getting more sophisticated
 - The impact of cyberattacks is getting larger
- *What will we do?*
 - *SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet*



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) | ■ BAS (Bulgaria) | ■ TUBITAK (Turkey) |
| ■ Vrije Universiteit (NL) | ■ TU Vienna (Austria) | ■ FORTH – ICS (Greece) |
| ■ Institute Eurecom (FR) | ■ Chalmers U (Sweden) | |

- 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.

SysSec Aim and Objectives (I)

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.

SysSec Aim and Objectives (II)

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.

SysSec Aim and Objectives (III)

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.

SysSec Aim and Objectives (IV)

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**.
 - **1st SysSec Workshop, July 6th 2011, Amsterdam, VU**
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.

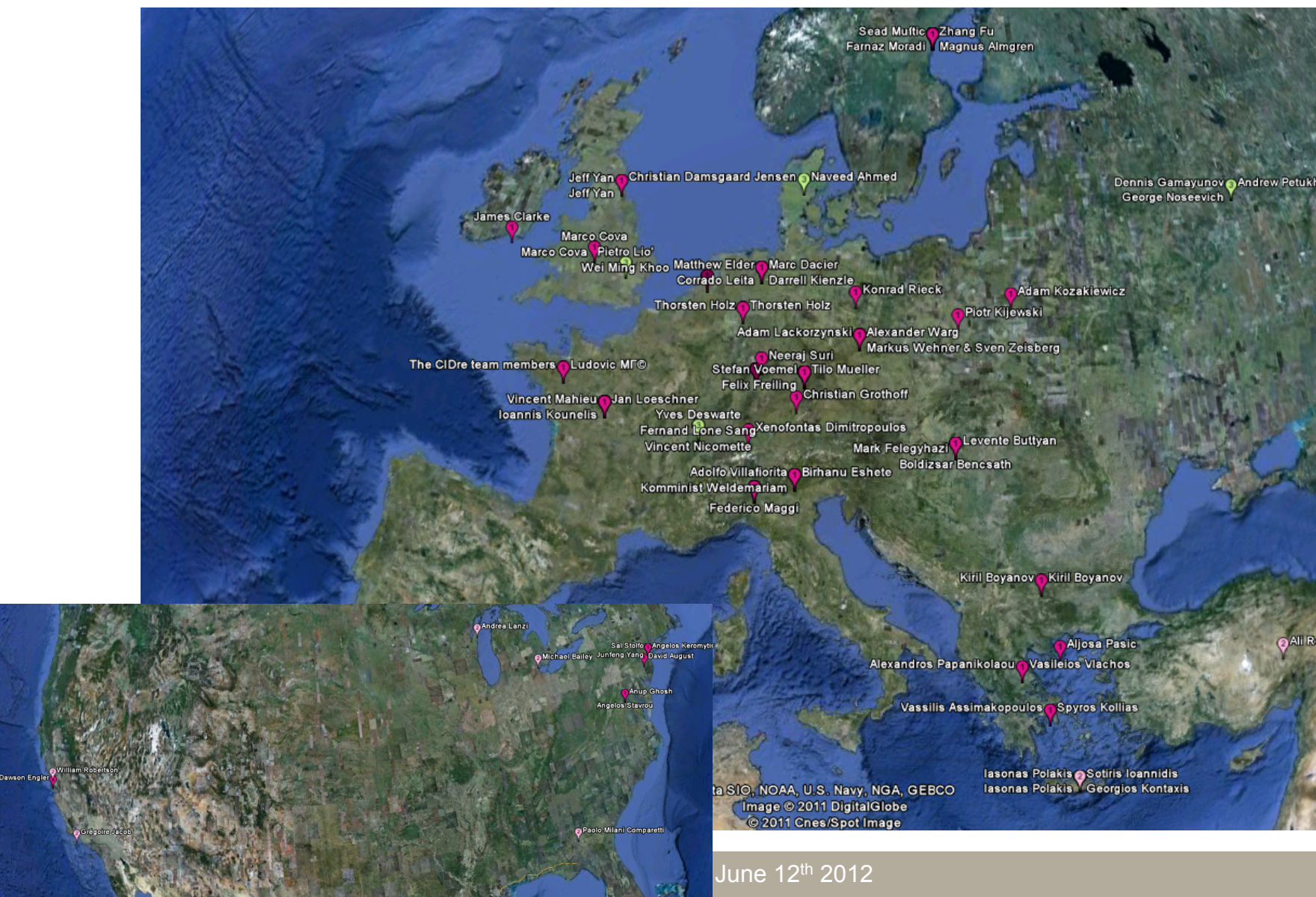
1st SysSec Workshop

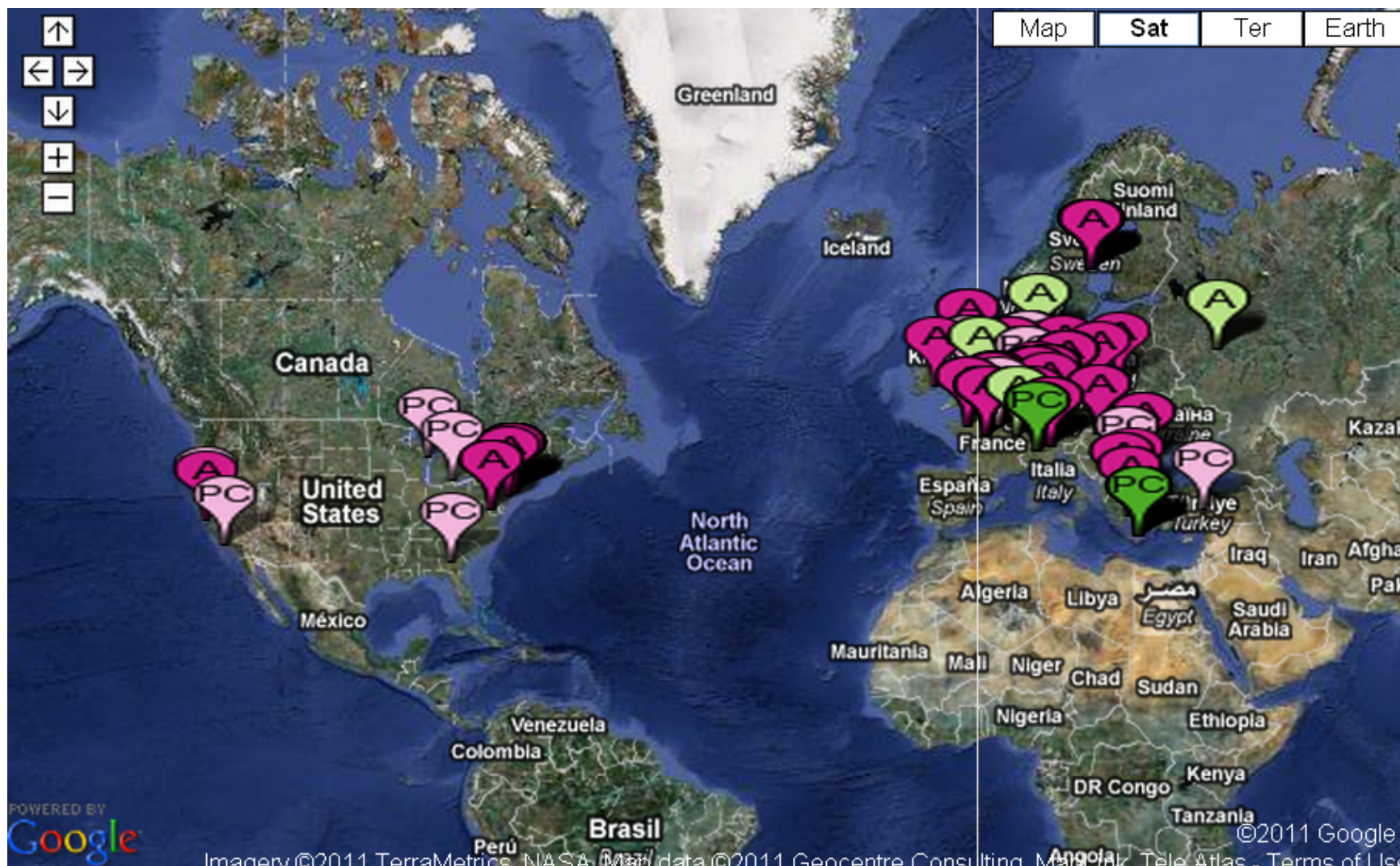
- By the numbers:
 - 23 **position** papers
 - i.e. where is the security research going?
 - 6 (longer) **Student/Research** papers
 - 95 authors
 - 36 organizations
 - One session on INCO strategy
 - In trustworthy ICT
 - Organized by the BIC project

1st SysSec Workshop – Who?



1st SysSec Workshop – International?





Research Roadmap



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 1st 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

