Privacy-Preserving Social Plugins

Evangelos Markatos

FORTH-ICS and U of Crete, Crete Greece

in collaboration with

G. Kontaxis, M. Polychronakis and A. Keromytis

Columbia University

Work appeared in USENIX SECURITY

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 are 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.

+1 +10 Recommend this on Google

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

More of what I "like"

DIMVA2012

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

+1 +2 Recommend this on Google

Like 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!

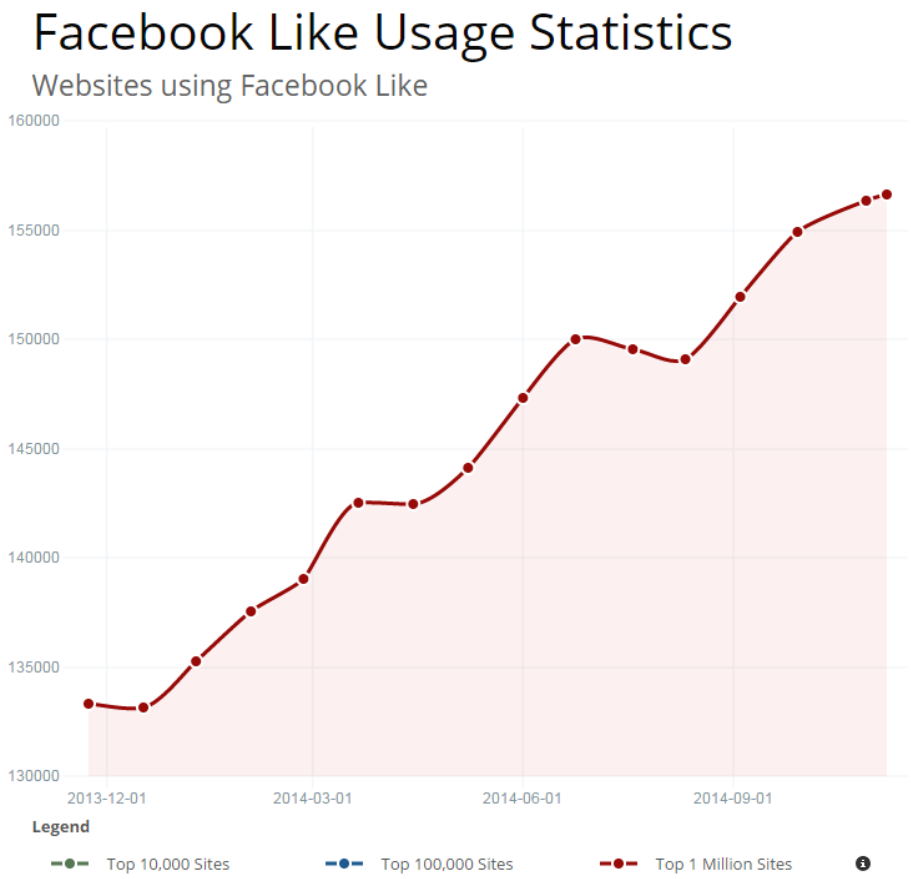
All our tweets.

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?

What is the extent of the problem?



- >15% of the top 1million Web sites include the "like" button
- ~30% for the top 10K sites
- Data from http://trends.builtwith.com/widgets/Facebook-Like

So

- 1 out of 3 to 1 out of 6 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

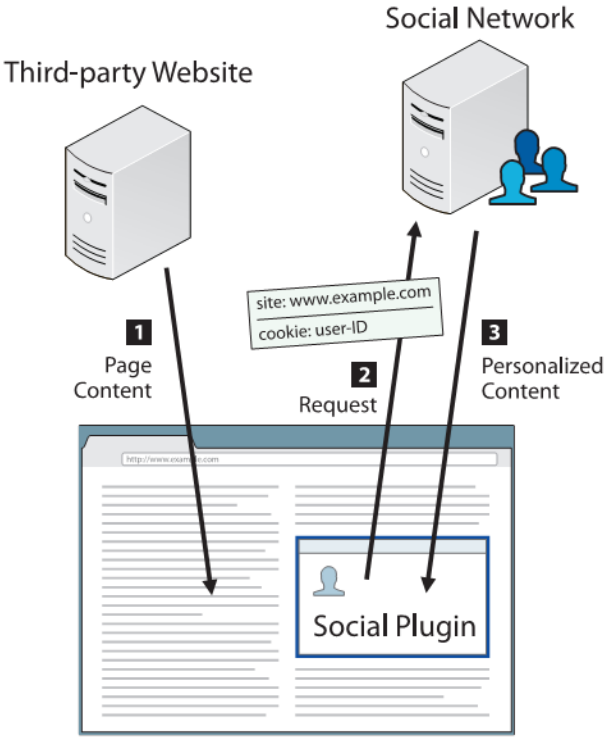
The code:

```
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
```

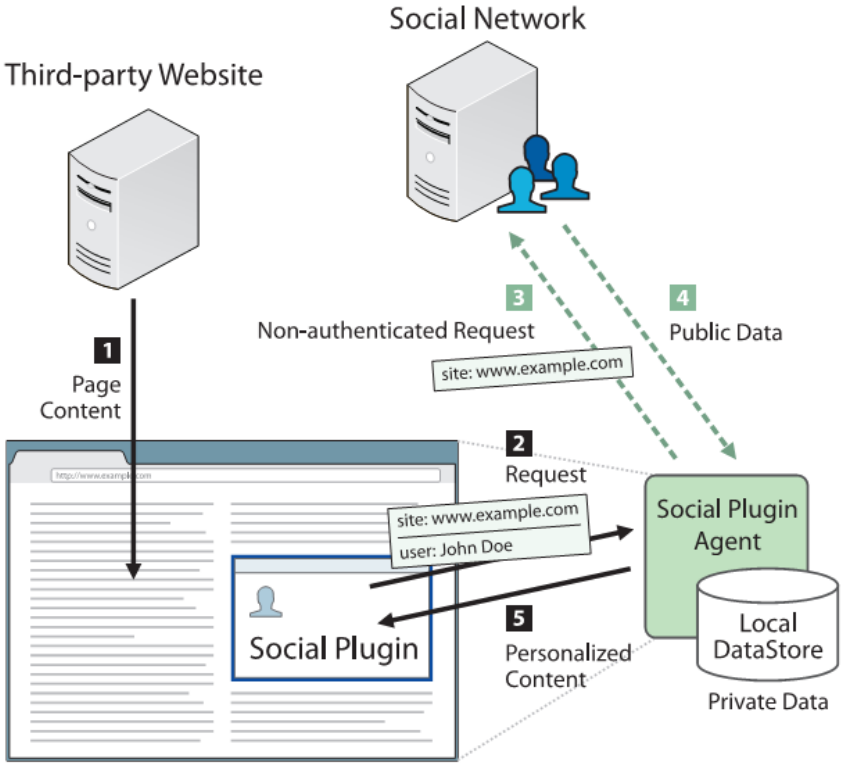
Listing 1. HTTP GET request for loading a Facebook Like button.

The data flow

Before



After



SafeButton

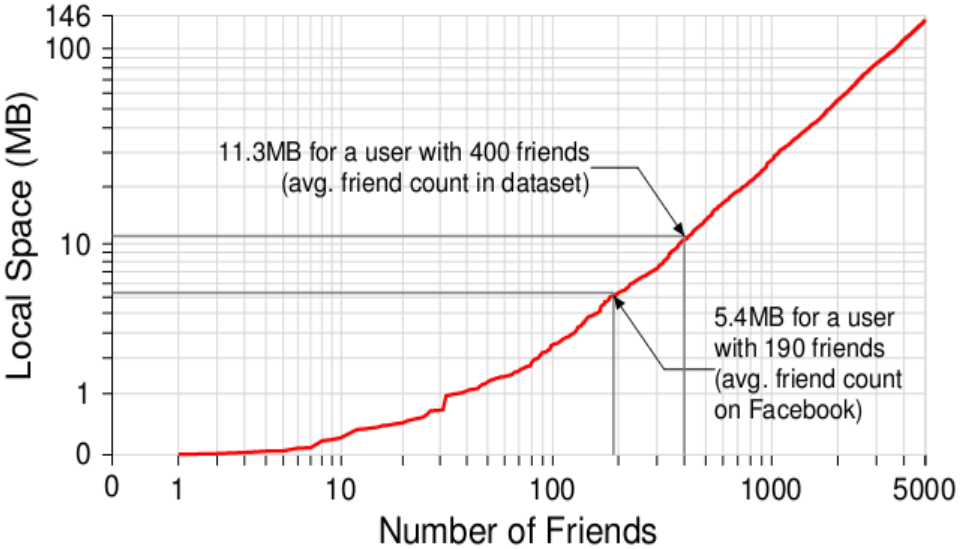
- Populating the local store with information.
- Social networks expose a developer's API.
  - Fetched information is data the user already has access to via his/her online profile.
- Instead of asking
  - (1) "has user Bob liked page A?"

    we ask
  - (2) "give me all the likes user 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 ☺

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)*

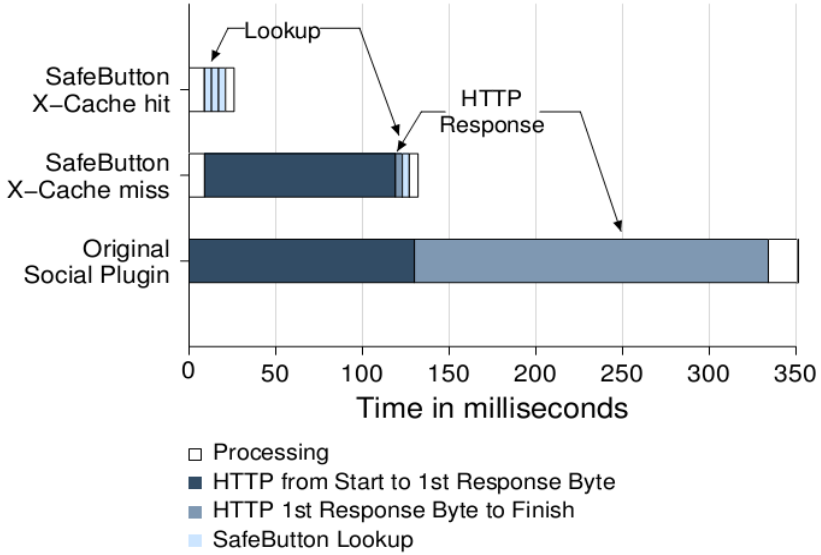


Fig. 7. Detailed timeline of the events taking place to load and fully render render a Like button with and without SafeButton.

Summary

- Social Networks change their business model
  - To become the single personalization and authentication service on the Internet
- Erosion of privacy
- Social Networks may 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

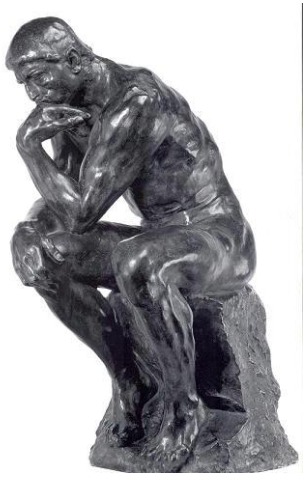
G. Kontaxis, M. Polychronakis and A. Keromytis

Columbia University

Work appeared in USENIX SECURITY

Hot topics in Security Research – the Red Book

Evangelos Markatos
FORTH-ICS



RoadMap of the talk

- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

RoadMap of the talk

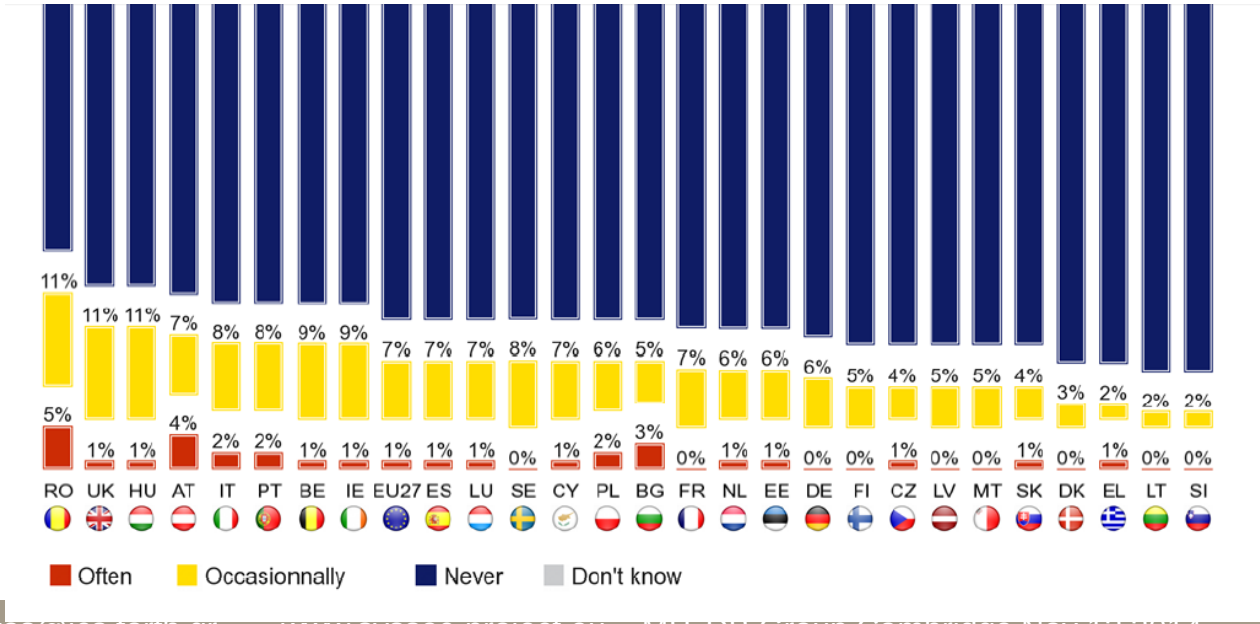
- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

Cyber Security is increasingly important

- The European Cyber Security Agenda:
  - 148,000 computers compromised daily
  - Symantec suggests that
    - Cybercrime victims lose 290 billion euros annually
  - 18% of users are less likely to buy goods online
  - 74% agreed that the risk of becoming a victim of cybercrime has gone up in the past year

Cyberattacks are getting more prelavent

- Hackers are getting more effective
- Users are getting more concerned
  - 12% of Internet users has experienced fraud
  - 8% have been victims of ID theft
    - » (src: Eurobarometer 390)



What is the impact of attacks?

"… potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: no more electricity or water at home, rail and plane accidents, hospitals out of service"

Viviane Reding

VP of the European Commission

European Cybersecurity Month

"in tomorrow's world if the internet isn't secured, nothing will be …"

Neelie Kroes

VP of the European Commission

How large is it?

- Cybercrime is *larger than*
  - *The global black market in marijuana, cocaine and heroin combined*

--Symantec

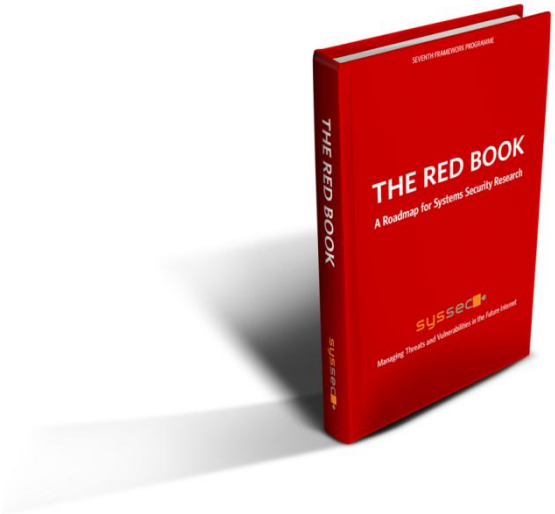
RoadMap of the talk

- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

What shall we do?

- *Understand the important Research Issues*
- *Write them down in a book*
- *Circulate it widely*
  - *So that researchers can work on them*

- *The result:*
  - *The Red Book*
    - *in Cyber Security*



RoadMap of the talk

- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

How did we do it?

- To build a winning team you need
  - Excellence,
  - Talent, and
  - Desire to work hard.

We assembled a Task Force of young European Researchers

Task Force

MEMBERS

Elias Athanasopoulos
Columbia University
Federico Maggi
Politecnico di Milano
Asia Slowinska
Vrije Universiteit

Lorenzo Cavallaro
Royal Holloway University of London
Michalis Polychronakis
Columbia University and FORTH
Iason Polakis
FORTH and University of Crete





Contributors

Magnus Almgren
Chalmers
Sotiris Ioannidis
FORTH
Philippas Tsigas
Chalmers
Herbert Bos
Vrije Universiteit
Christian Platzer
TUV
Stefano Zanero
Politecnino di Milano

CONTRIBUTORS

Dennis Andriesse
Vrije Universiteit
Farnaz Moradi
Chalmers University
Simin Nadjm-Tehrani
Linköping University
Martina Lindorfer
TU Vienna
Zlatogor Minchev
Bulgarian Academy of Sciences
Christian Rossow
Vrije Universiteit

Chairs

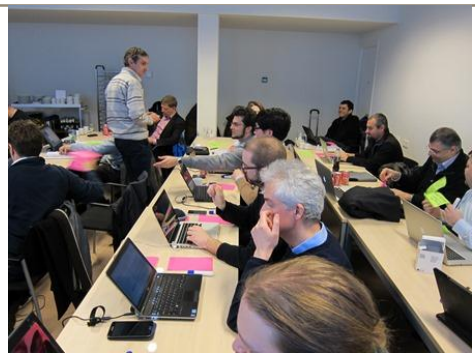
SYSSEC TASK FORCE for the ROADMAP on SYSTEMS SECURITY RESEARCH

CO-CHAIRS

Evangelos Markatos
SysSec Project Manager
Foundation for Research and Technology - Hellas

Davide Balzarotti
SysSec WP4 Leader
Eurecom

The making of Red Book



- "Rank the threats" workshop
  - Which are the important threats?
  - Rank them
- "What if" questions
- Grand Challenges

RoadMap of the talk

- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

“What if” Questions

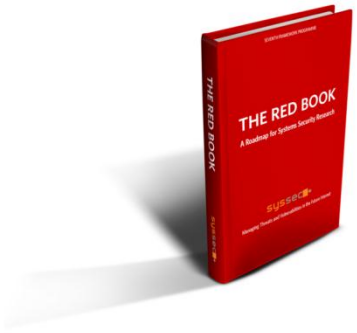
- Examples from other disciplines
  - What if …
    - Antibiotics do not work anymore?
      - How would this impact medicine research?
    - There are no more fossil fuels to burn in 5 years?
      - How would this impact research in energy sources?
- “What if” questions
  - What if there is no more malware?
  - What if 50% of the computers are compromised?
  - What if there is no death? (for our data)
  - What if there is no Internet? (for a day or two)

“What if” Questions

- What if there is no more malware?
  - Will Security Research be over?
  - Will there be any security issues?
  - How about privacy issues?
- What if 50% of the computers are compromised?
  - How would you use them?
    - Why? When?
  - Would you do e-banking?
    - Under what circumstances?

“What if” Questions

- What if there is no death? (for our data)
  - Can we donate them?
  - Can we pass them on to our children?
- What if there is no Internet? (for a day or two)
  - What would work? What would not work?
  - Traffic? Air travel?
  - Will you be able to go home?
    - From work? from a business meeting?



Example “what if”

- What if there is no death? (for our data)
  - Will they be available after we pass away?
  - Can our children “inherit” our data?
    - Will they be able
      - to “own” our data?
      - to pass them on to the next generation?
        - » much like family photo albums?

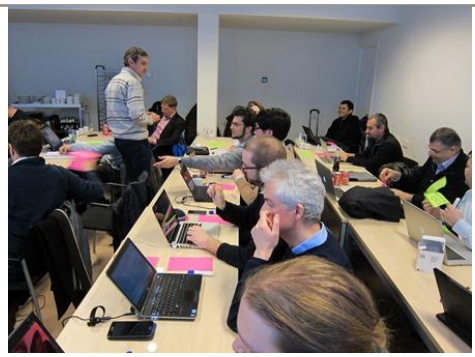
  - Can we donate our data?
    - to Science?
    - Are there any security/privacy implications?
  - Can we incorporate all our data to an avatar?
    - Will the avatar be able to act on behalf of us?

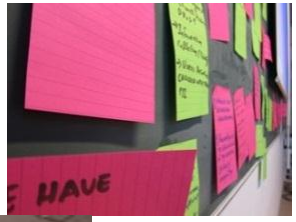
RoadMap of the talk

- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

The Threats

- "Rank the threats" workshop
  - Which are the important threats?
  - Rank them

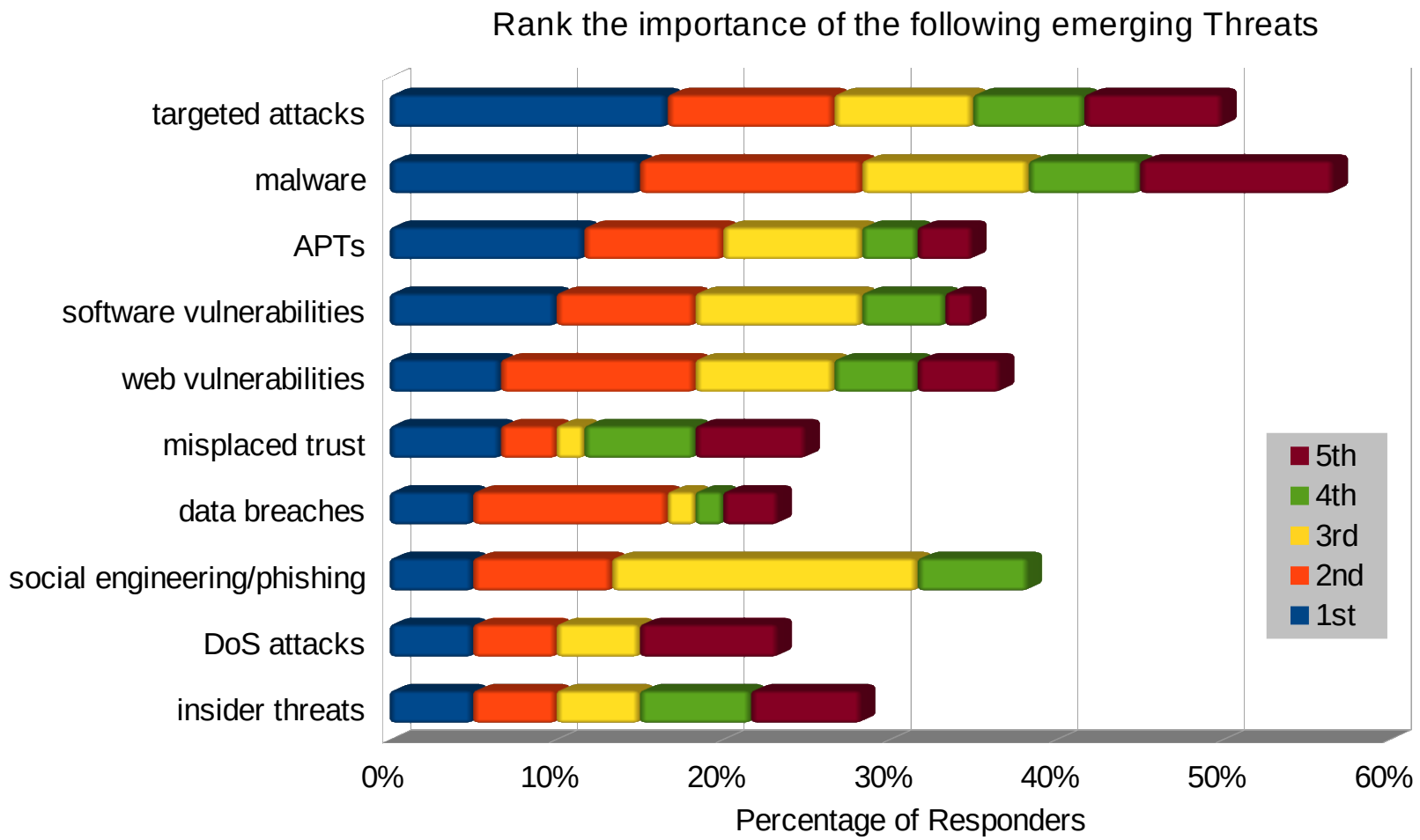




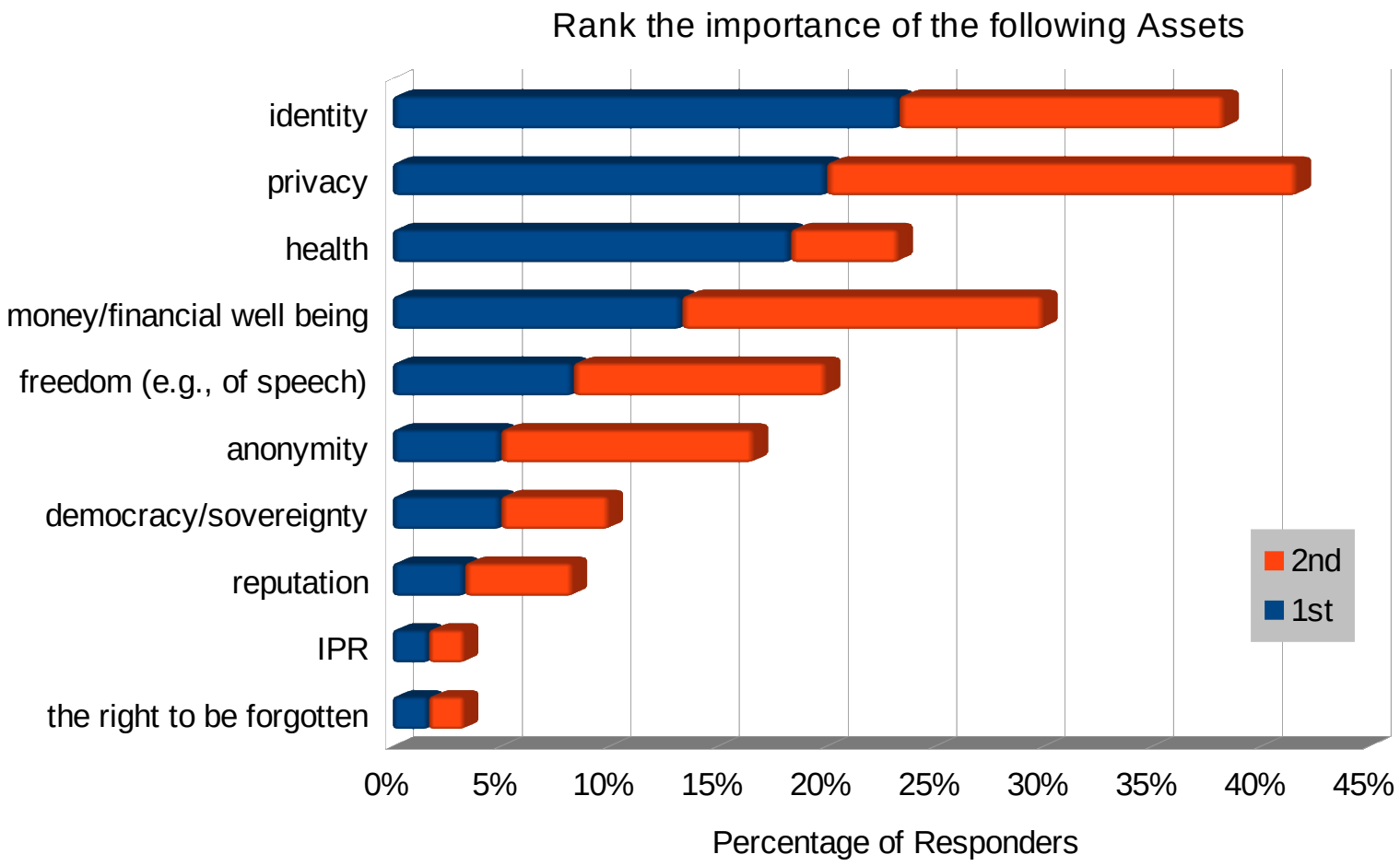
Cyber-security landscape

- Threat – Vulnerabilities
- Assets
- Domains
- Horizontal Research Areas

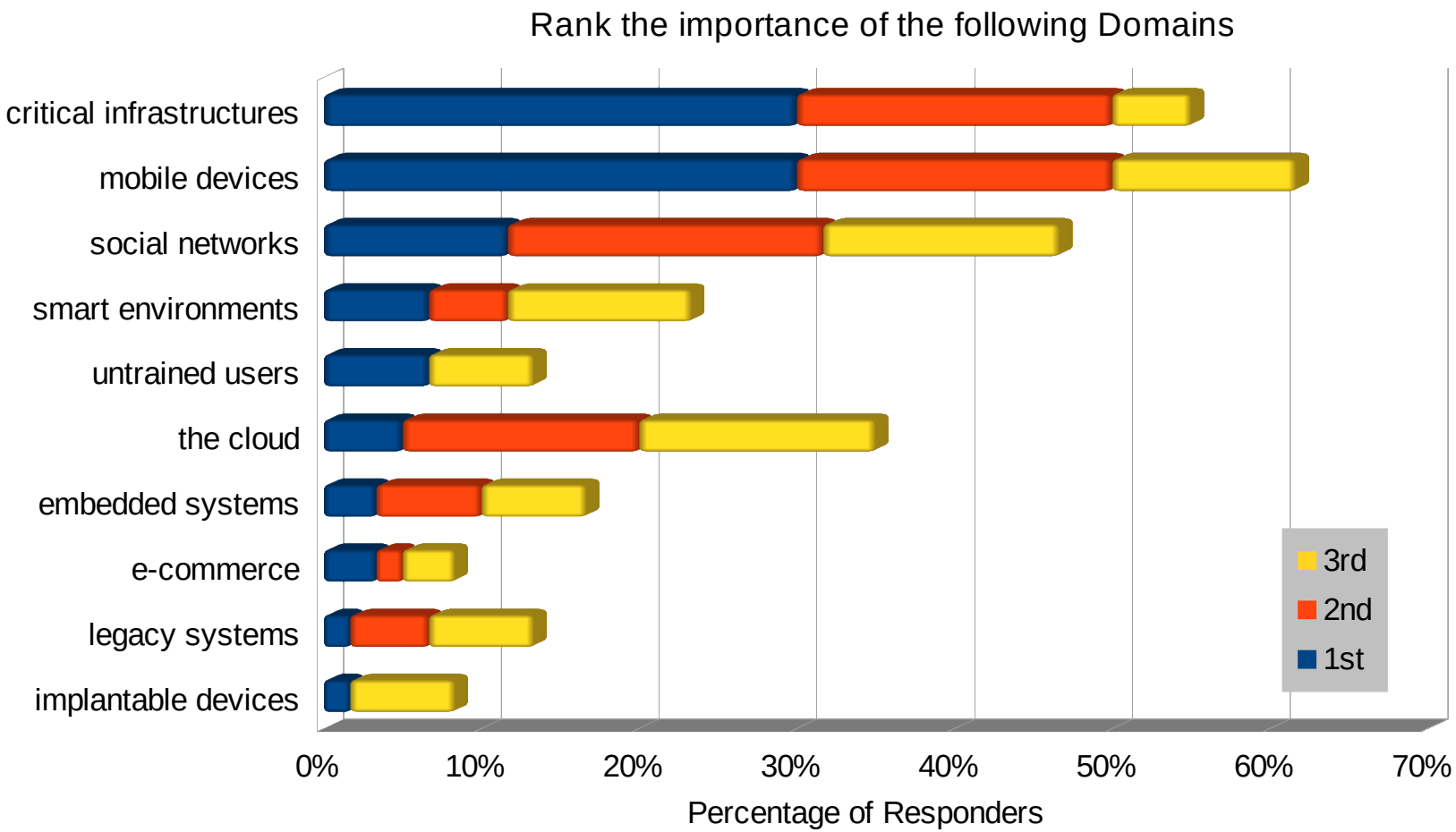
Threats - Vulnerabilities



Assets


Rank the importance of the following Assets
identity
privacy
health
money/financial well being
freedom (e.g., of speech)
anonymity
democracy/sovereignty
reputation
IPR
the right to be forgotten
2nd
1st
0%
5%
10%
15%
20%
25%
30%
35%
40%
45%
Percentage of Responders

Domains


Rank the importance of the following Domains
critical infrastructures
mobile devices
social networks
smart environments
untrained users
the cloud
embedded systems
e-commerce
legacy systems
implantable devices
3rd
2nd
1st
0%
10%
20%
30%
40%
50%
60%
70%
Percentage of Responders

Most important threats

- Malware
- Targeted Attacks – Advanced Persistent Threats
- Social Engineering - Phishing

RoadMap of the talk

- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

Grand challenges

- No device should be compromisable
- Give users control of their data
- Provide private moments in public places
- Develop compromise-tolerant systems

Example Grand Challenge

- Give users control over their data
- Users should be able to
  - know which data they have created
  - know which data they have given to which third parties
    - Cookies, accesses, IP addressses, MAC addresses, etc.
  - Revoke all access to their data
  - Ask data to be deleted
    - if this is not prohibited by law

RoadMap of the talk

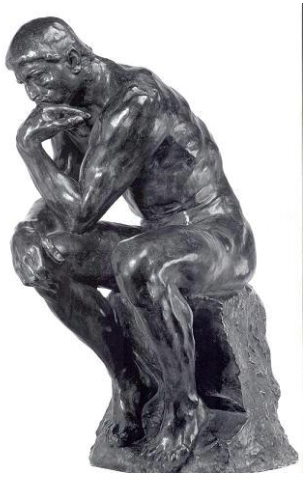
- Introduction
- The Red Book
- The making of the Red Book
- “What if” Questions
- The Threats
- The Grand Challenges
- Summary

Summary

- The Red Book:
  - Identify Research Directions in Systems Security
- The making of it:
  - Task Force of young excellent scientists
    - They drive the work
  - Workshop with the community
    - Everyone engaged
- The result:
  - Threats, assets, priorities
  - Grand Challenges

Hot topics in Security Research – the Red Book

Evangelos Markatos
FORTH-ICS



WP4: Research Roadmap