FIRE

Gateway to trustworthy ICT innovations in Europe

Supported under:

SEVENTH FRAMEWORK PROGRAMME

Hot topics in Security Research – the Red Book

Evangelos Markatos

FORTH

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

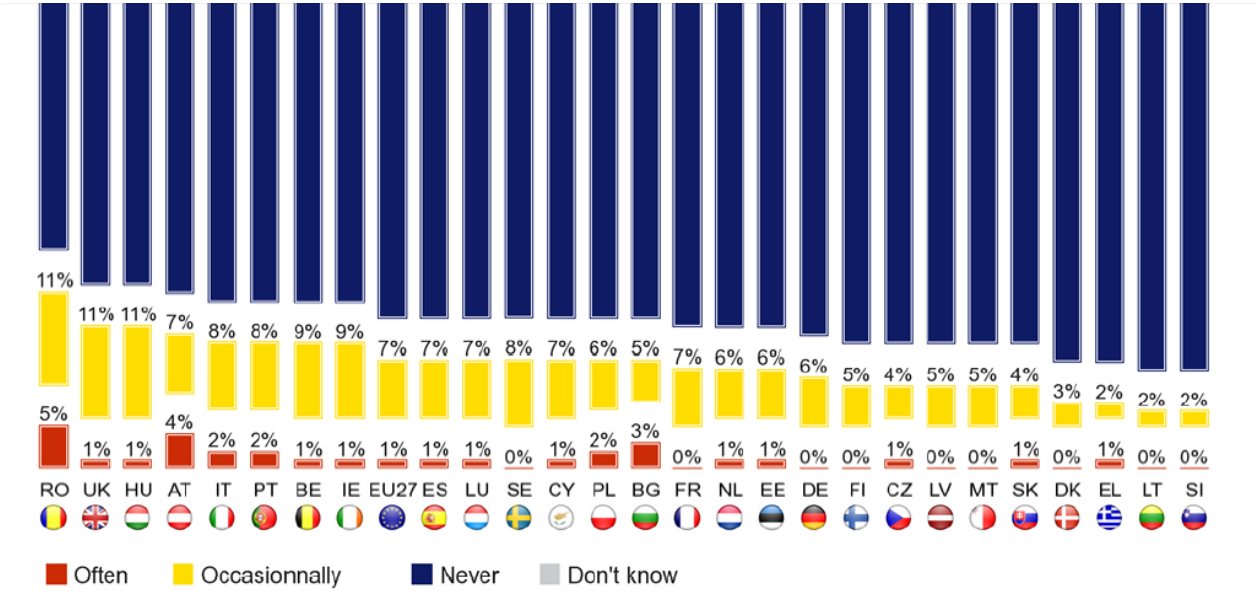
Cyber Security is increasingly important

- 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

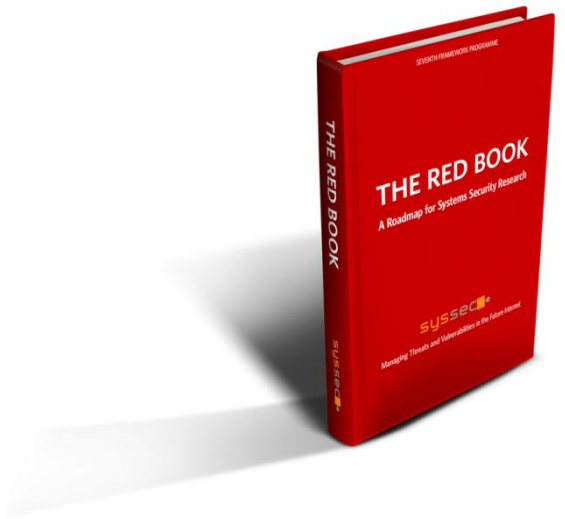
RoadMap of the talk

- 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

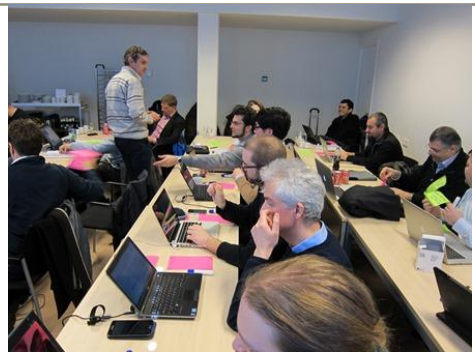
SYSSEC TASK FORCE for the ROADMAP on SYSTEMS SECURITY RESEARCH

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”

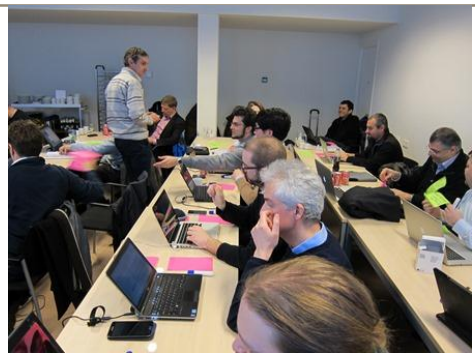
- What if there is no death? (for our data)
  - Will they be available after we pass away?
  - Can our children “inherit” our data?
    - Will they be able
      - to “own” our data?
      - to pass them on to the next generation?
        - » much like family photo albums?
  - Can we donate our data?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

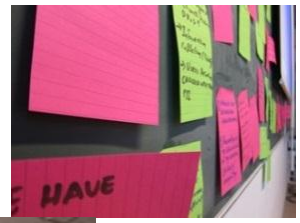
RoadMap of the talk

- 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

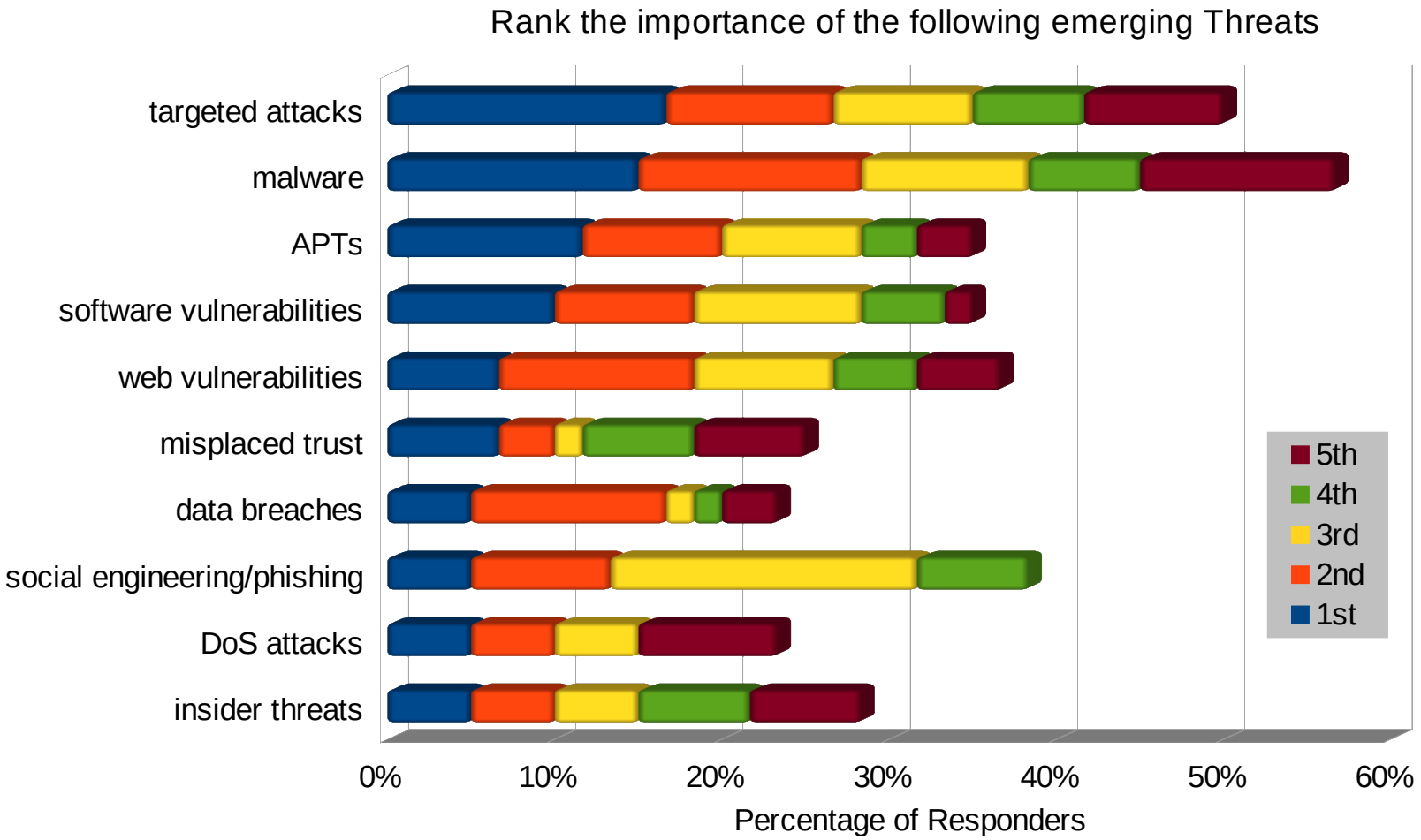




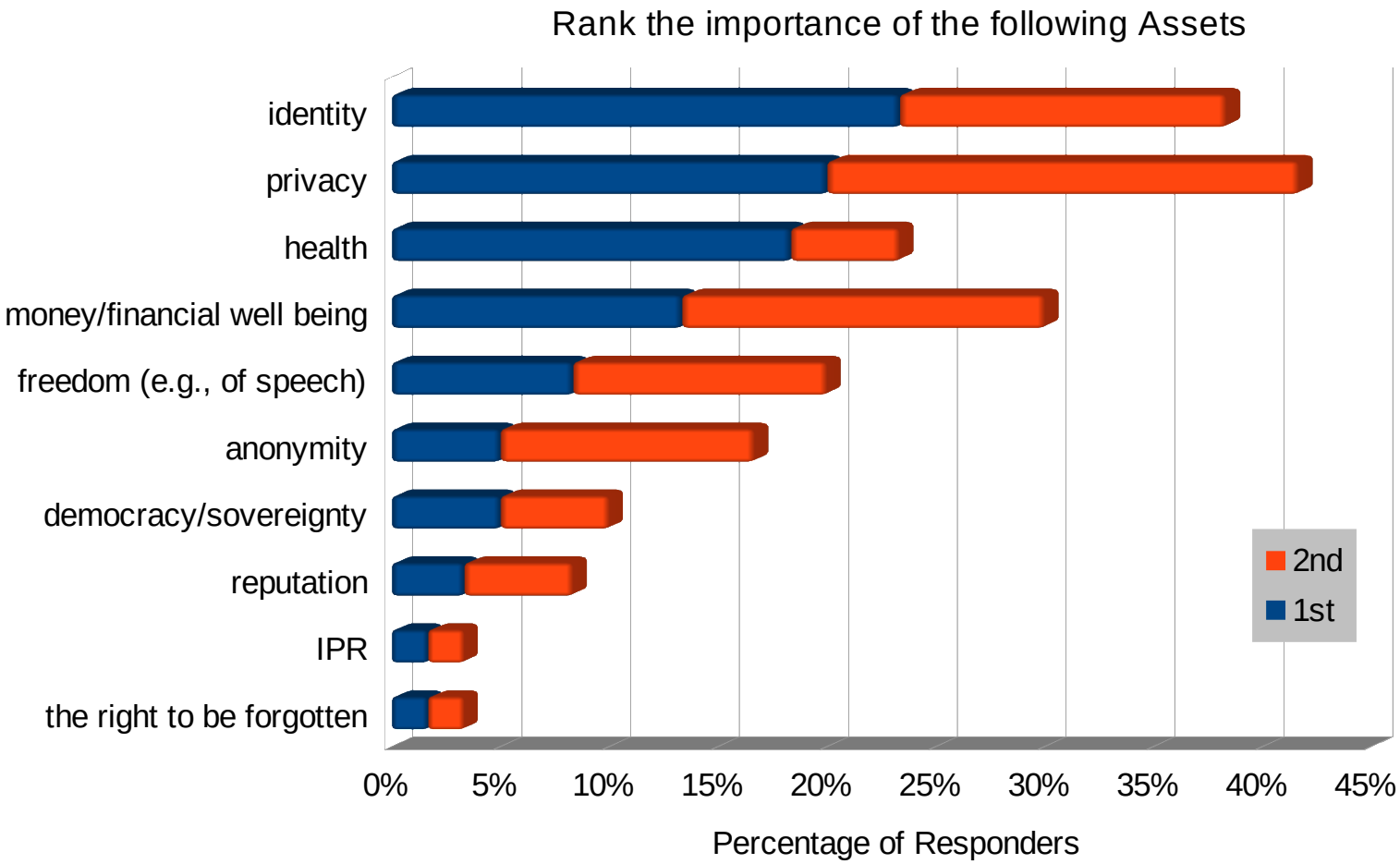
Cyber-security landscape

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

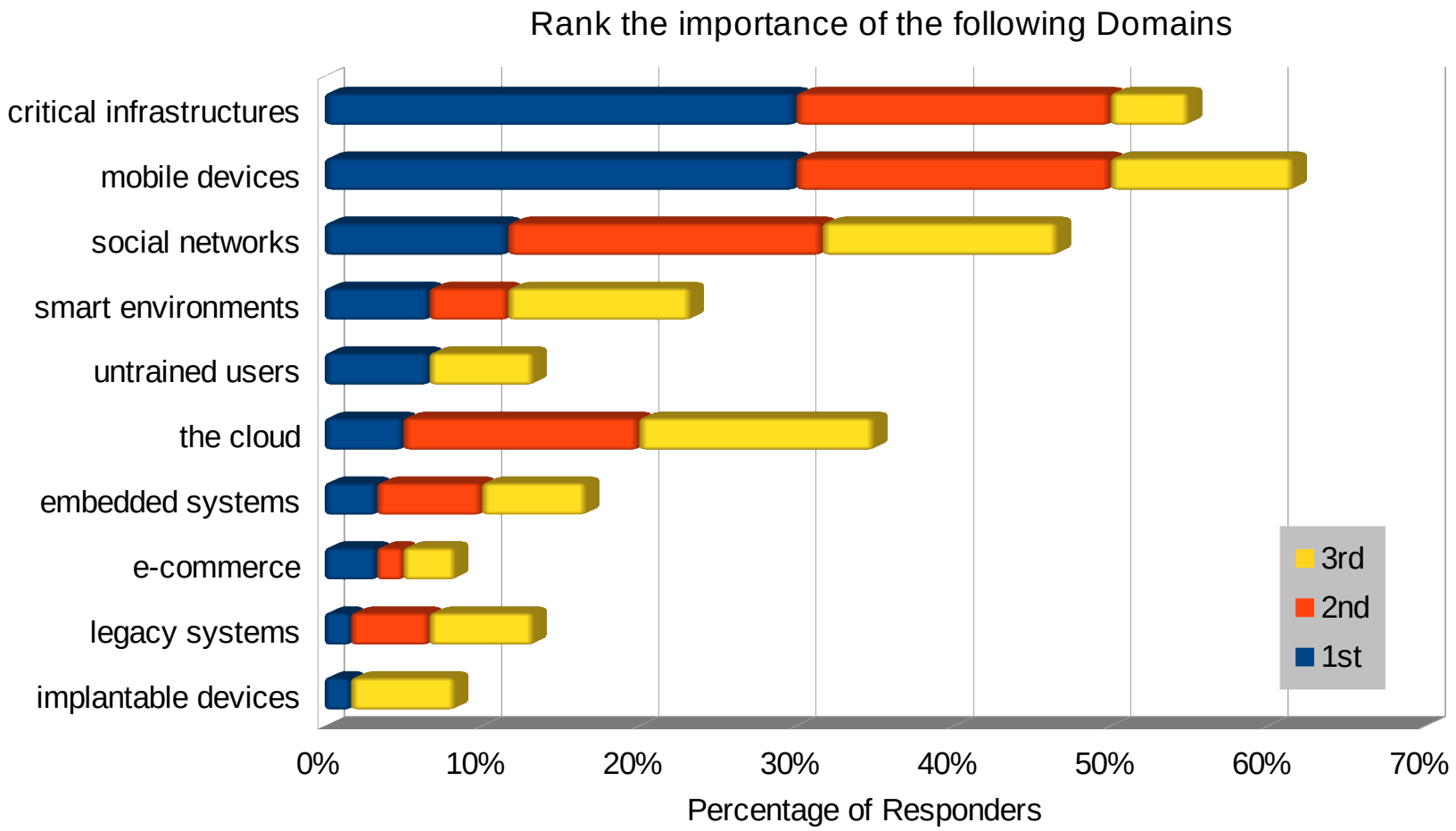
Threats - Vulnerabilities



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

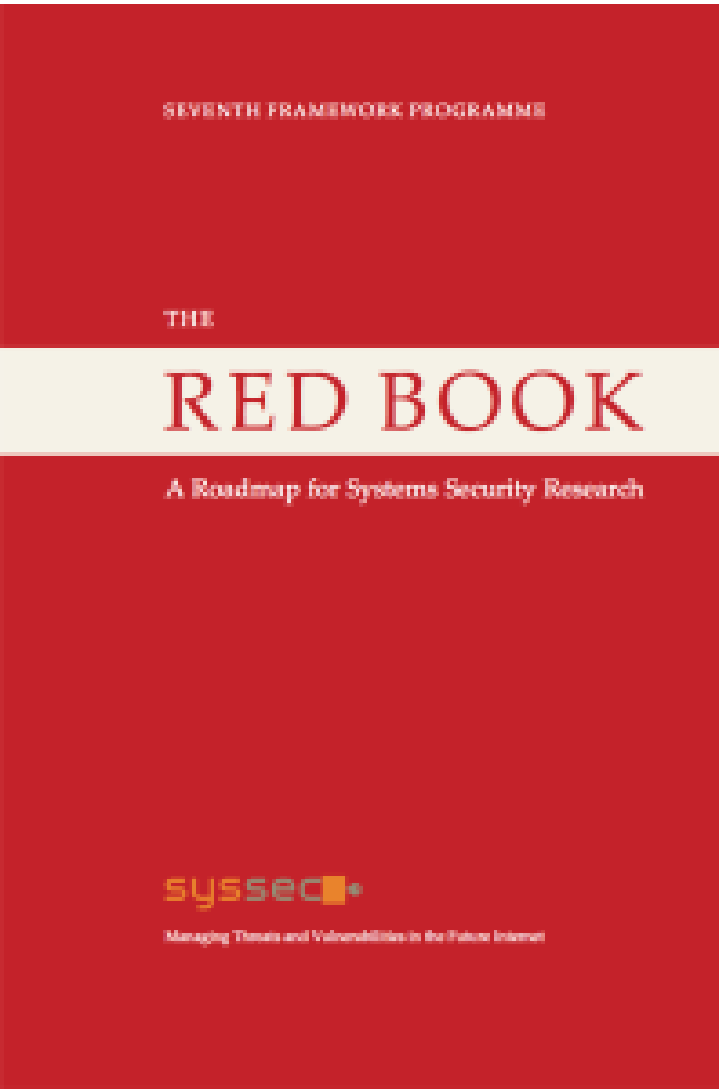
Summary

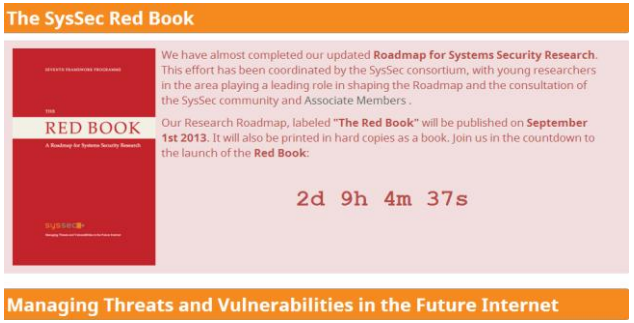
- The Red Book:
  - Identify Research Directions in Systems Security
- The making of it:
  - Task Force of young excellent scientists
    - They drive the work
  - Workshop with the community
    - Everyone is engaged
- The result:
  - Threats, assets, priorities
  - Grand Challenges

Hot topics in Security Research – the Red Book

Evangelos Markatos
FORTH-ICS

WP4: Research Roadmap





Panel Questions

- Biggest concerns:
  - End user
    - Losing control of their data
      - and their identity
  - State-sponsored espionage
    - States have the resources needed to launch
      - Sophisticated attacks
      - Difficult to protect against

Panel Questions

- Do we need to be concerned?
  - Users: Yes
    - What if your favorite cloud provider is hacked and hackers threaten to expose all your data?
      - Business plans?
      - Confidential information? Such as medical/legal?
  - Business: Yes
    - Business will not boom if your users do not trust you
    - Would customers buy form you if you
      - Do not replace lost/stolen shipments?
      - Do not refund unwanted shipments?
      - Do not deliver purchased goods?

Panel Questions

- Role of policy makers:
  - Regulation for apps
    - Disclose what data they collect and what they do with it
  - Force apps to work with minimum information
    - Currently apps request access to a lot of data
      - If the user does not give access – they just do not work
      - Apps should provide service even with minimal data
        - » Even if the user refuses cookies

Top 3 innovations

- Give users control over their data
  - Who has which data for which user
    - Names, IP addresses, cookies, browser fingerprints, etc.
- Provide a liability framework
  - If an app steals my money/data, who is responsible?
- Anonymization/Obfuscation
  - Provide the minimum amount of data
    - That still allows decent functionality
      - e.g. obfuscate GPS coordinates

Priorities 2015+

- Give back users the control of their data
- Privacy in public places
- Anonymization – Obfuscation