Security and Privacy Research Challenges
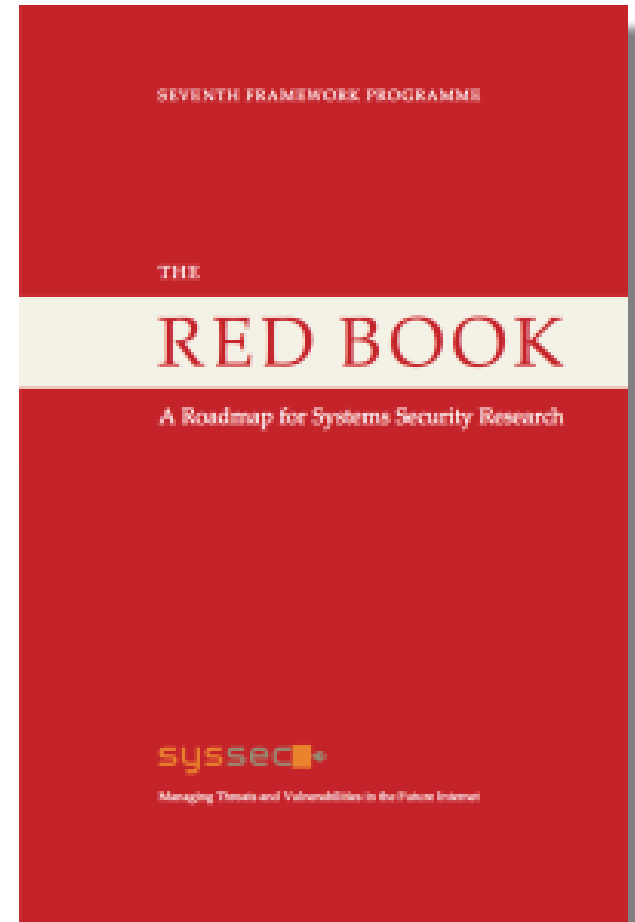
Sotiris Ioannidis

Institute of Computer Science

Foundation for Research and Technology - Hellas

Red Book

- The Red Book of System Security
    - Results of an extensive survey among security experts
    - 11 threats described in details
    - 4 grand challenges
    - 10 chapters covering previous roadmaps and recommendations
    - 2 appendixes covering methodologies and threat landscape evolution

SEVENTH FRAMEWORK PROGRAMME

THE

RED BOOK

A Roadmap for Systems Security Research

syssec

Managing Threats and Vulnerabilities in the Future Internet

Red Book [target audience]

- Policy Makers
  - The Executive Summary provides a high-level overview of the book content
  - Separate chapter dedicated to the Grand Challenge Research Problems that call for the collaboration of several Research Organizations and the support of leading funding Agencies
- Researchers
  - Both young and experienced researchers can find something useful in the book
  - Examples of Ph.D. topics are proposed at the end of each chapter
- Journalists
  - Average and worst case scenarios for all the covered emerging threats
  - This can help journalists raising the public awareness for these threats without underestimating or overplaying their impact

Red Book [the making of]

- ## Who?
  - Red Book task force
  - Three Syssec Working Groups
  - Associated members of SysSec
  - More than 30 security-related EU projects
  - Broader Systems Security Community

- ## How?
  - Plenary face-to-face meeting in Amsterdam
  - Online survey
  - Feedback from other projects

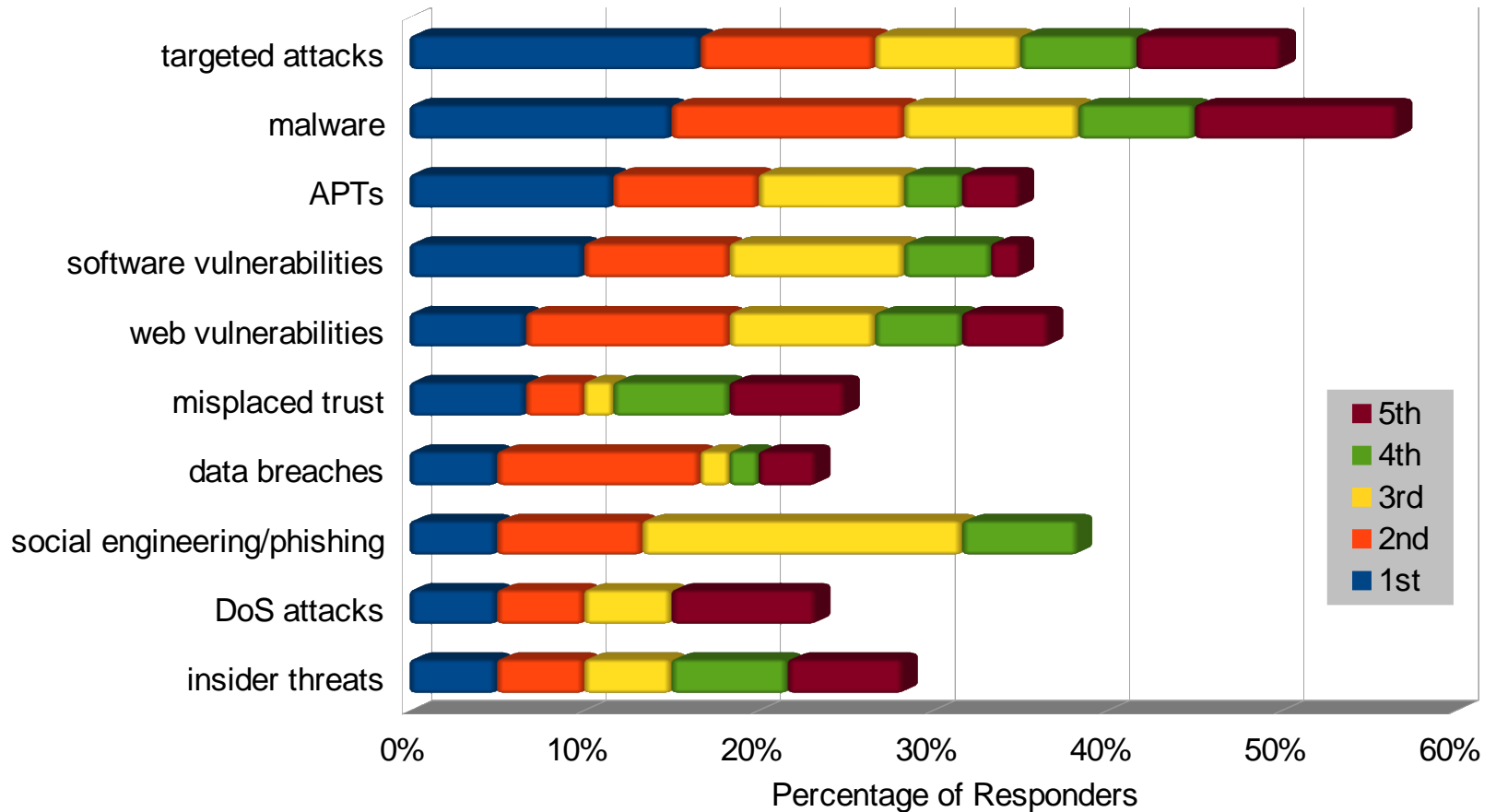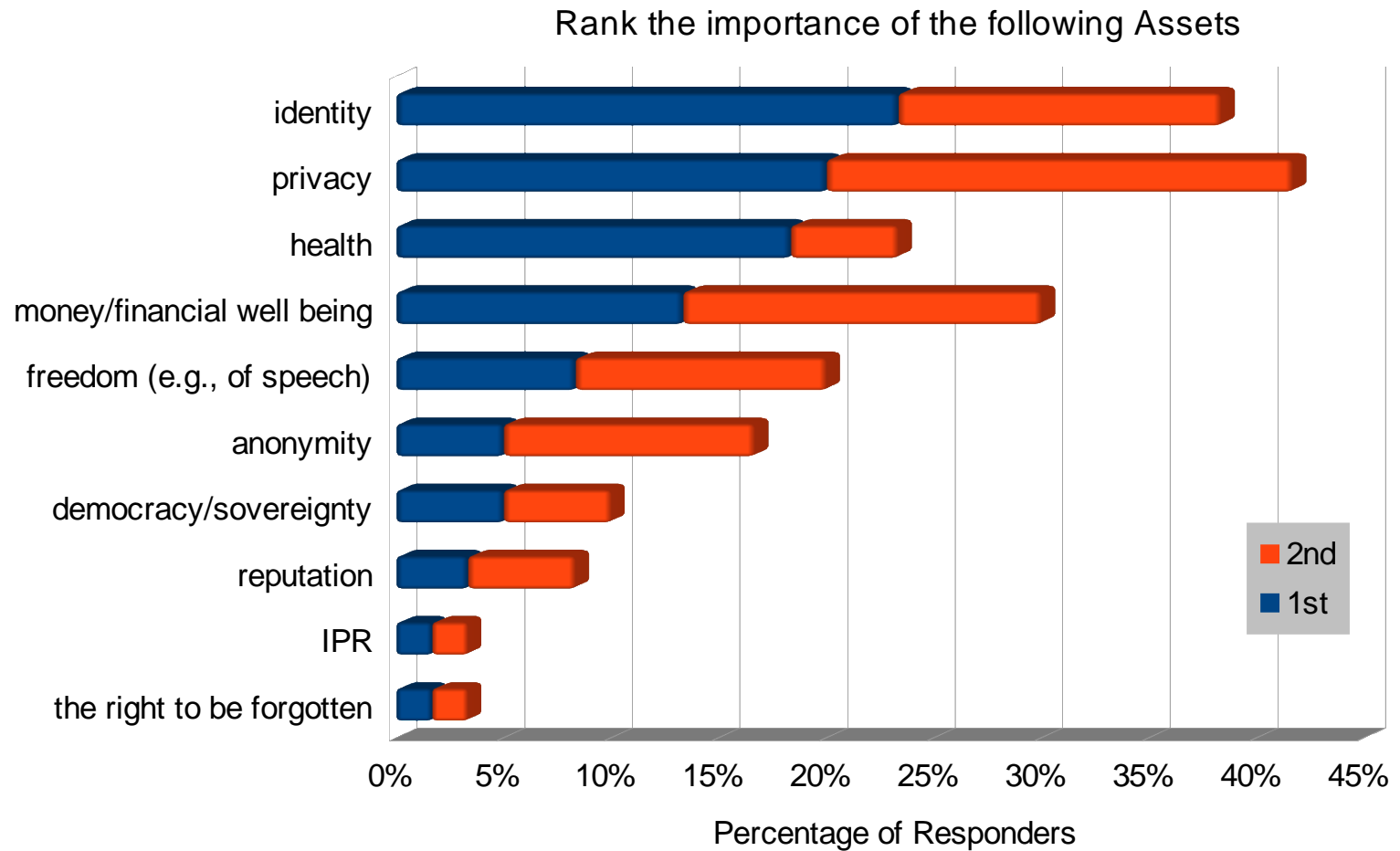# Cyber-security landscape

- Threat – Vulnerabilities

- Assets

- Domains
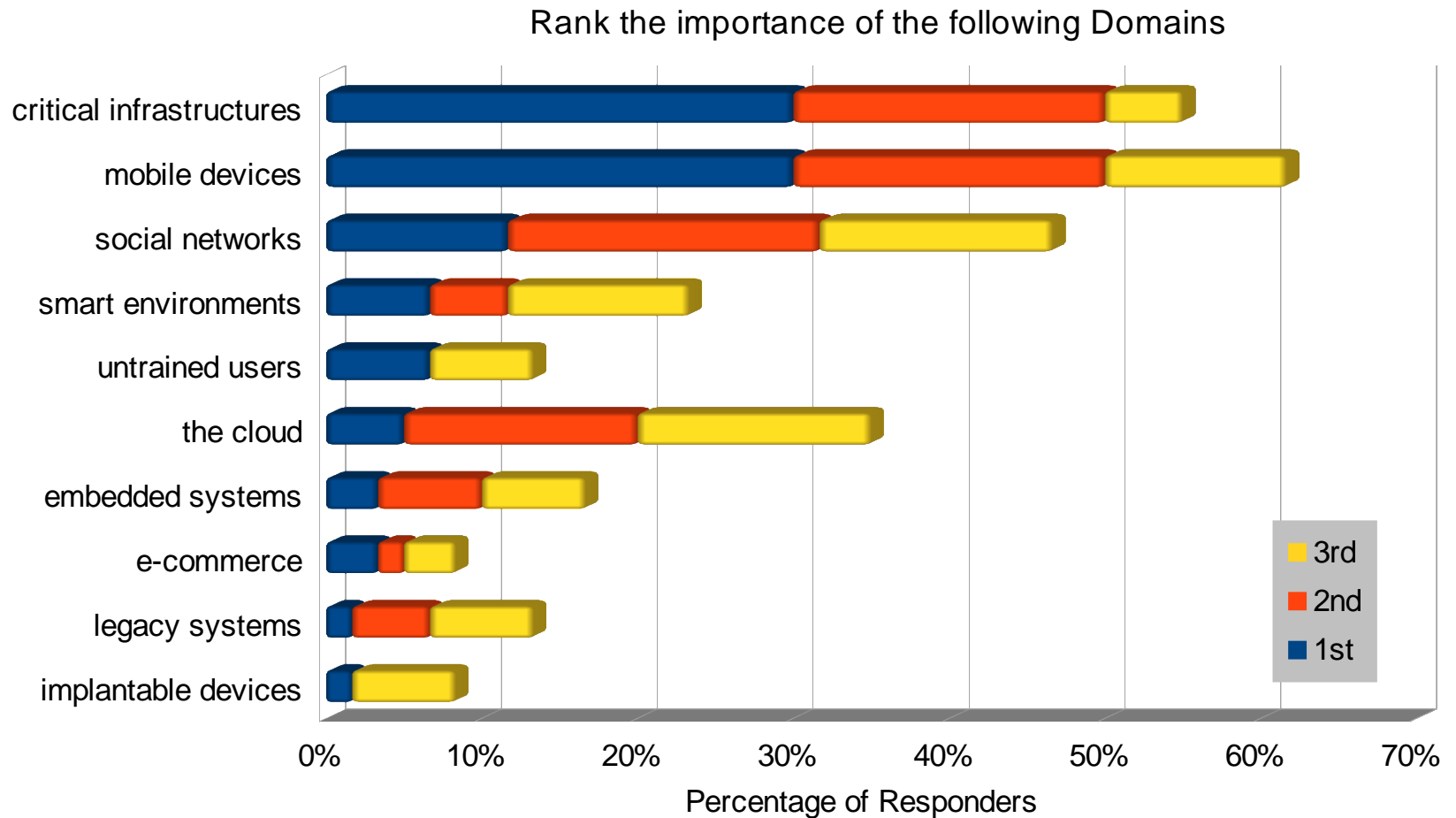
- Horizontal Research Areas

Threats - Vulnerabilities

Rank the importance of the following emerging Threats

Assets

Rank the importance of the following Assets

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

Legend: 3rd, 2nd, 1st

Percentage of Responders

Most important threats

- Malware

- Targeted Attacks – Advanced Persistent Threats

- Social Engineering - Phishing

Major challenges

- No device should be compromisable

- Give users control of their data

- Provide private moments in public places

- Develop compromise-tolerant systems

Priorities

- Invest in usable and practical security

- Develop systems with measurable security properties

Conclusions

- syssec-project.eu

- red-book.eu