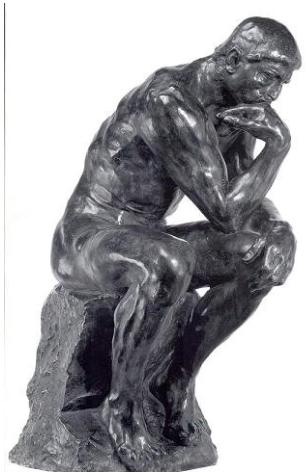
Building cybersecurity research capabilities: the European experiences of the SysSec and PROTASIS networks

Stefano Zanero
Politecnico di Milano



POLITECNICO DI MILANO

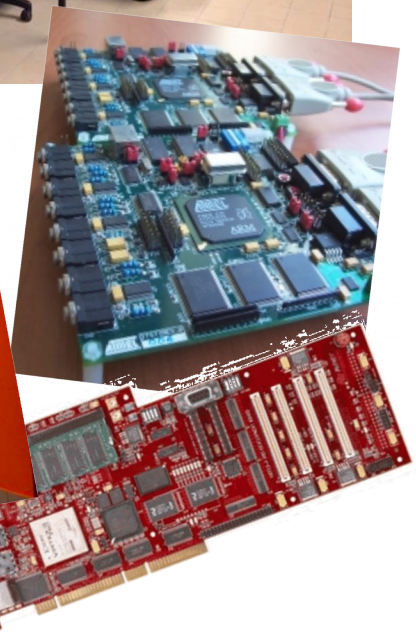
Professors and students 2014/15

	STUDENTS	PROFESSORS
ARCHITECTURE	8.329	342
DESIGN	3.853	97
ENGINEERING	27.739	858

	2015
QS World ranking Engineering & Technology	31
QS World ranking Engineering & Technology Employer reputation	4 (EE) 6 (CS)
Applications (BSc)	16.500
Foreign students (MSc)	23%
Funds on a competitive basis (millions €)	140+

NECSTLab @ Polimi

- ✓ Professors
  - Full: **4**
  - Associate: **8**
  - Assistant: **6**
- ✓ Thesis works: 50-60/year
- ✓ Class Projects: 80-100/year
- ✓ Post-Doc: **3**
- ✓ PhD Studenst: **12**
- ✓ Research Assistants: **9**

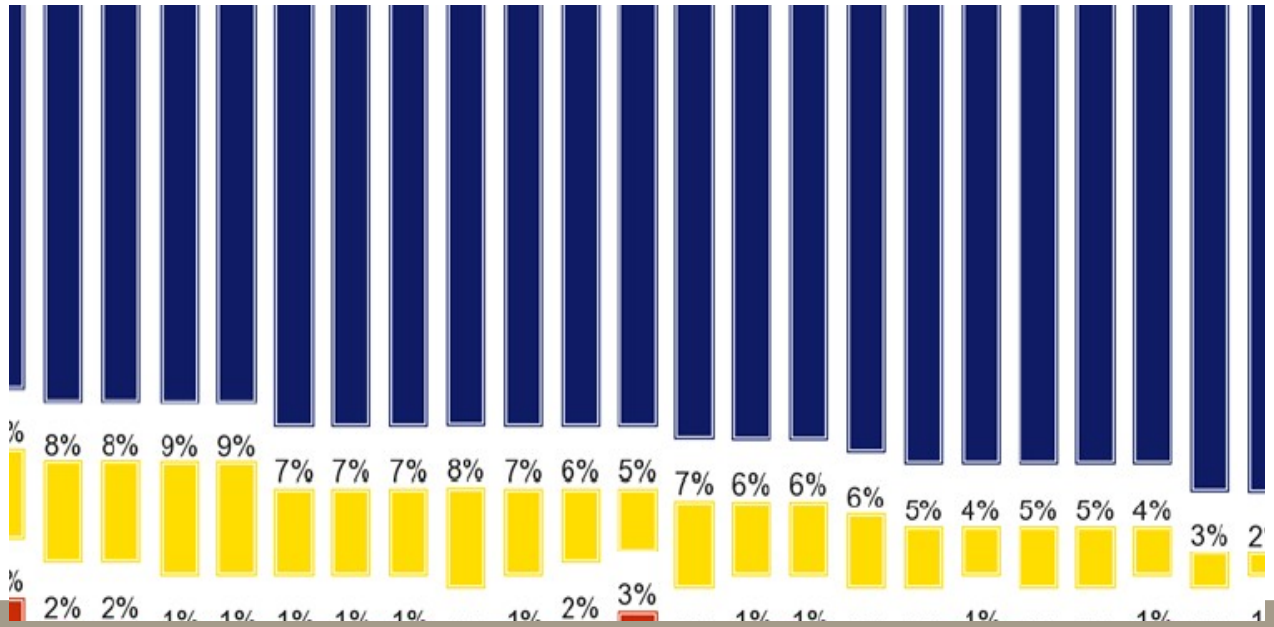


The problem we wished to address

- "Managing threats and vulnerabilities for the future Internet"
  - Attackers are getting more sophisticated
  - The attack surface is significantly increasing
    - Computers, smartphones, SCADA, Internet of Things
    - Adults, children, seniors
  - Users have started to feel the actual effects of the attacks
    - Fraud, ID theft, money loss

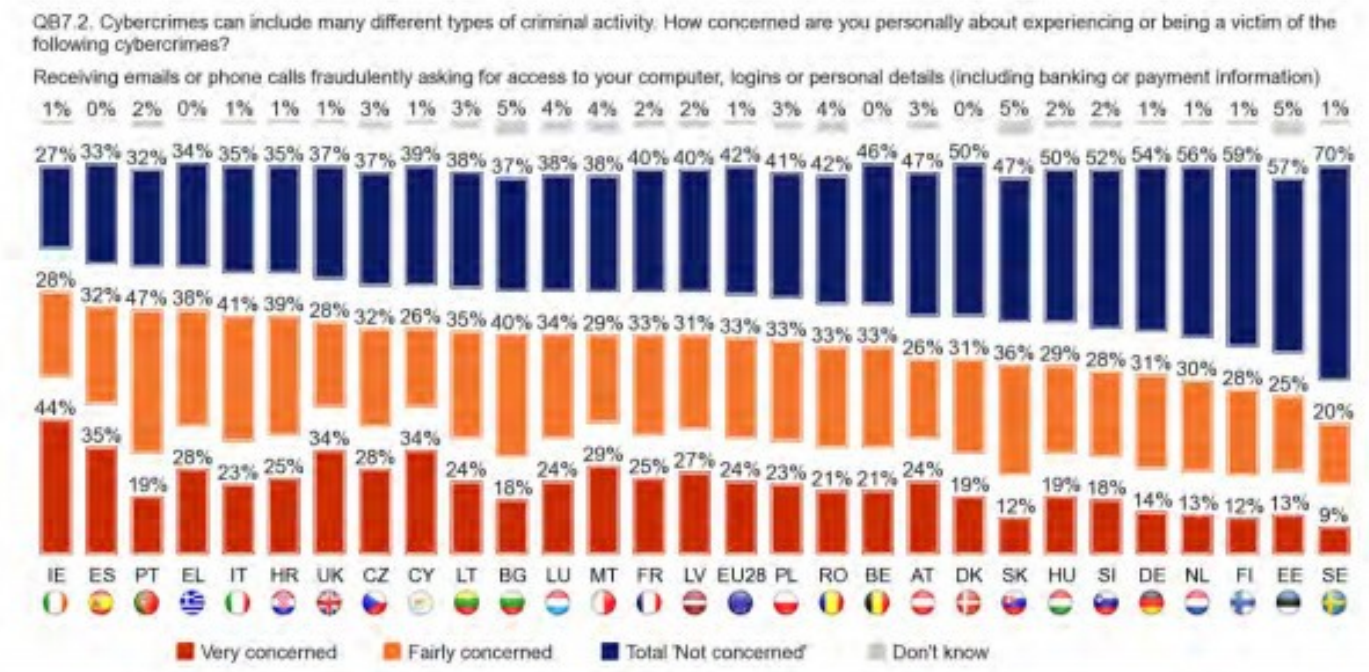
Cyberattacks are getting more prevalent

- 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)



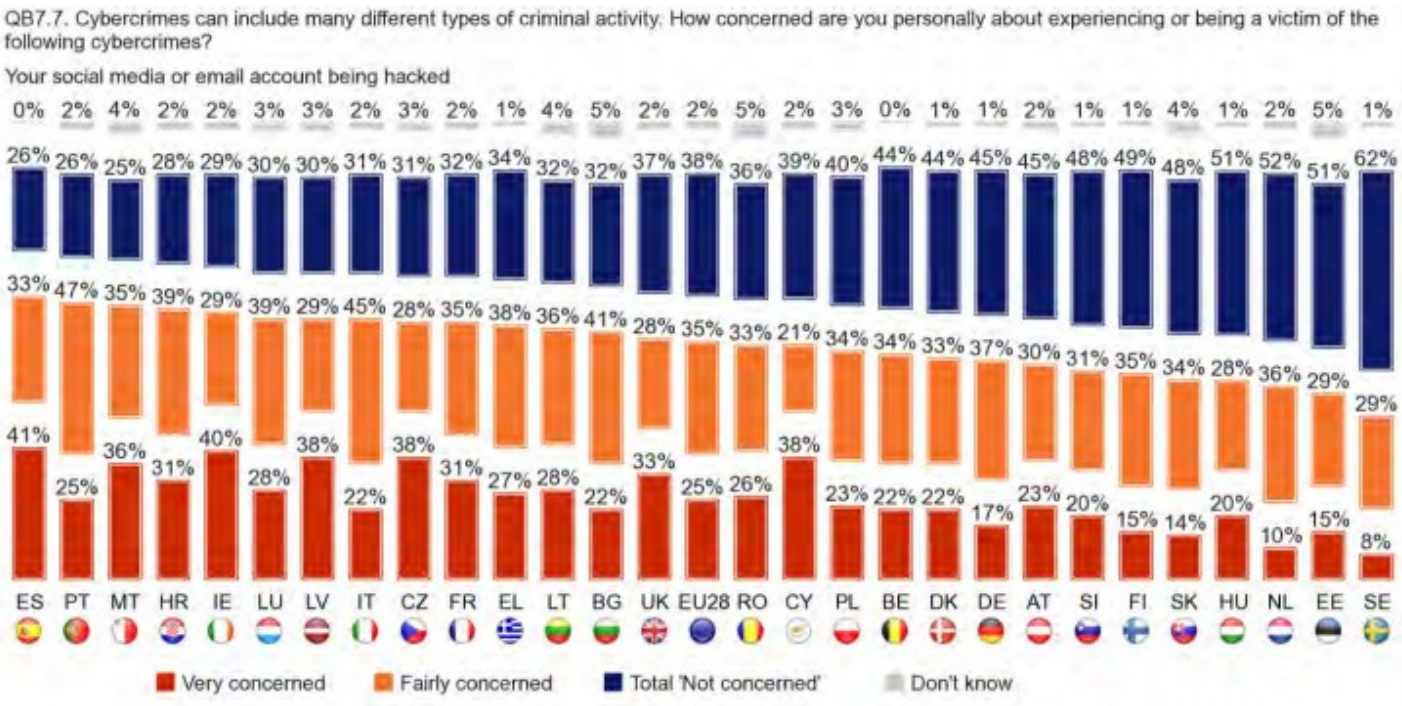
Cyberattacks are getting more prevalent

- 56% of Europeans are concerned
  - About on-line banking fraud
    - src: Eurobarometer 423 (October 2014)



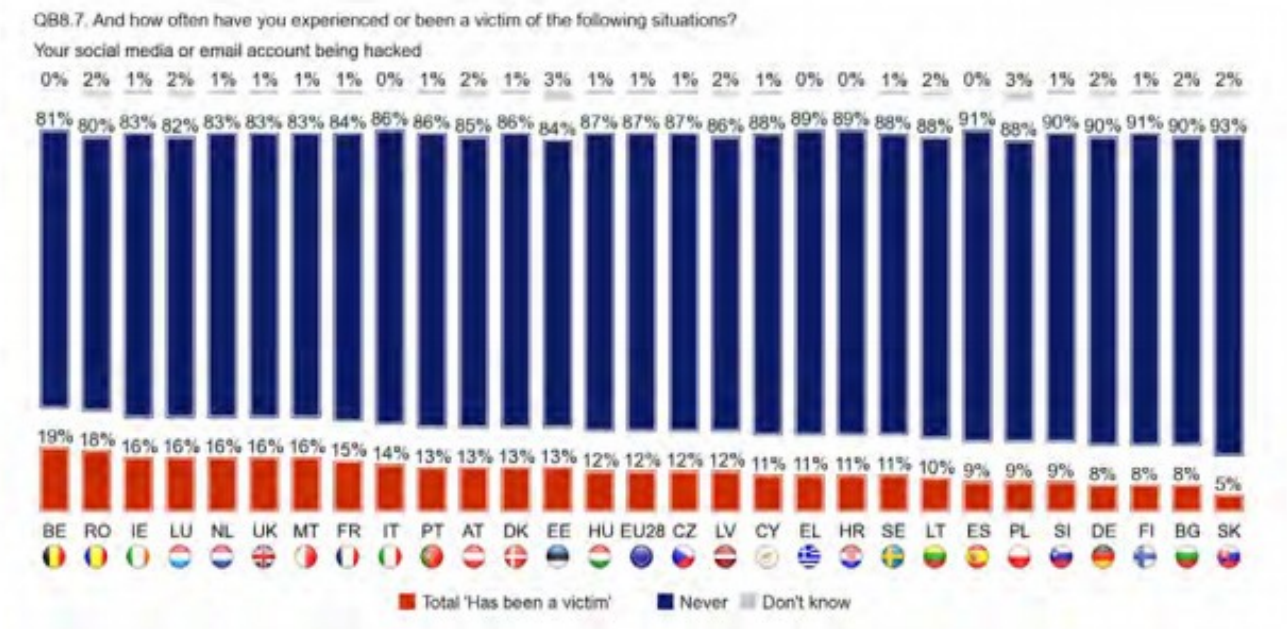
Cyberattacks are getting more prevalent

- 60% of Europeans are concerned
  - About their email account getting hacked
    - src: Eurobarometer 423 (October 2014)



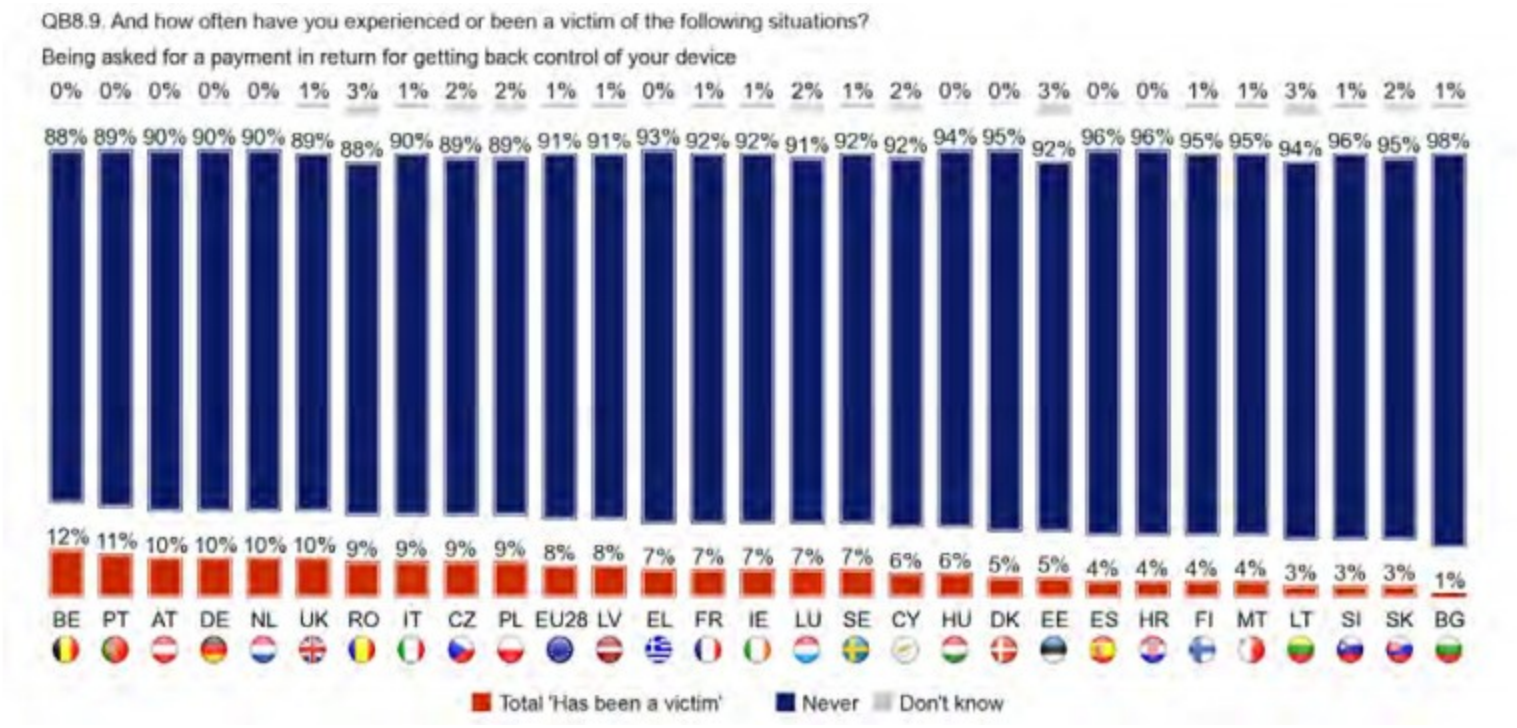
Cyberattacks are getting more prevalent

- 12% of Europeans reported that they
  - had their social accounts hacked
    - src: Eurobarometer 423 (October 2014)



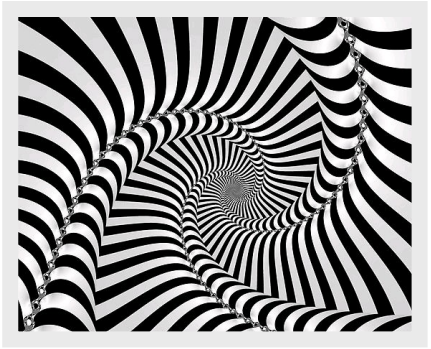
Cyberattacks are getting more prelavent

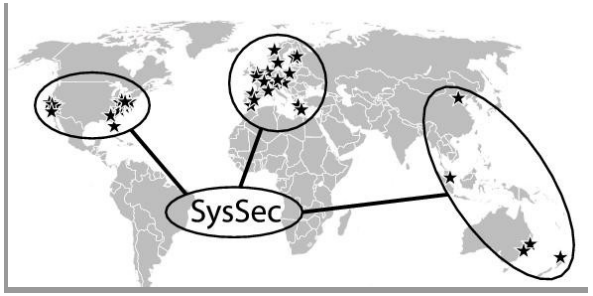
- 8% of Europeans have been blackmailed
  - Asked for payment to get back control of their device
    - src: Eurobarometer 423 (October 2014)



What we proposed with SysSec

- A Network of Excellence to implement a *game-changing* approach to cybersecurity:
  - Traditionally Researchers were mostly reactive:
    - they usually track cyberattackers *after* an attack has been launched
    - thus, researchers are always one step behind attackers
  - SysSec aimed 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.





The team

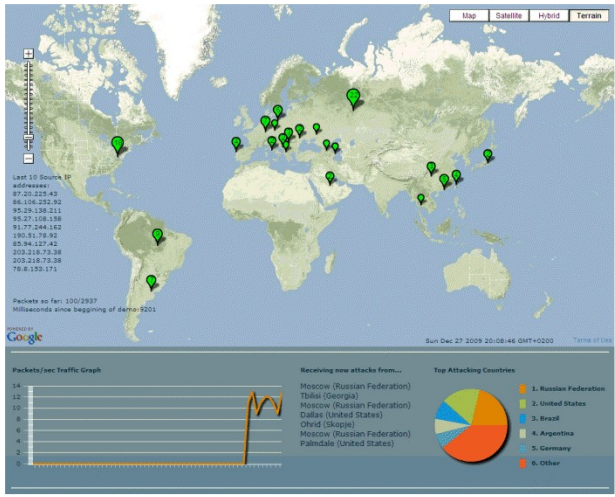
- Politecnico di Milano (IT)
- Vrije Universiteit (NL)
- Institute Eurecom (FR)
- IICT-BAS (Bulgaria)
- TU Vienna (Austria)
- Chalmers Univ. (Sweden)
- TUBITAK (Turkey)
- FORTH – ICS (Greece)

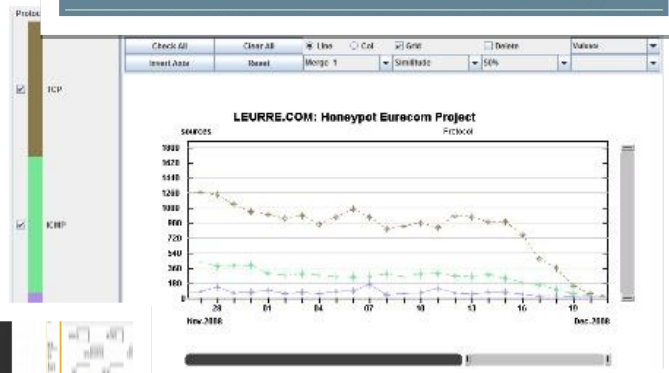
The partners: aggregating experiences

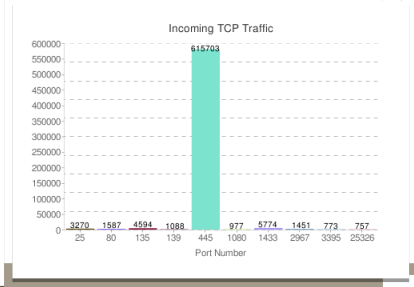
- Installed the largest honeypot infrastructure in Europe - among the leading in the World
  - Leurre com, SGNET, NoAH
    - >40 sensors in five continents, > 200.000 src IP addresses, >60.000 code injection attacks
- Built Argos: a pioneering emulator for capturing zero-day attacks
- Contribute to the development of WOMBAT: the first European cyberattack DataBase
- Mobilized FORWARD: the prominent European-led International think-tank on emerging threats
- Founded/Drive some of the largest European Systems Security Venues: ACM EuroSEC, DIMVA, RAID, etc.

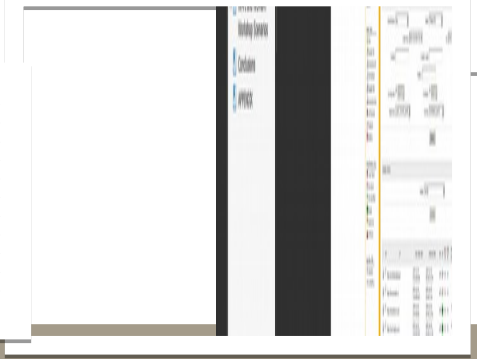
… and resources

- Existing sensors and honeypot infrastructures that collect cyberattack information
  - SGNET, leurre com, NoAH, etc.
    - >40 sensors in five continents, > 200.000 src IP addresses, >60.000 code injection attacks
- Incident data from these sources have been integrated within the WOMBAT ICT project database along with:
  - Honeyspider, wepawet, etc.
- Public-domain sources and through SysSec's world-wide constituency:
  - SANS.org, SPAMhaus, Offensive Computing, etc.







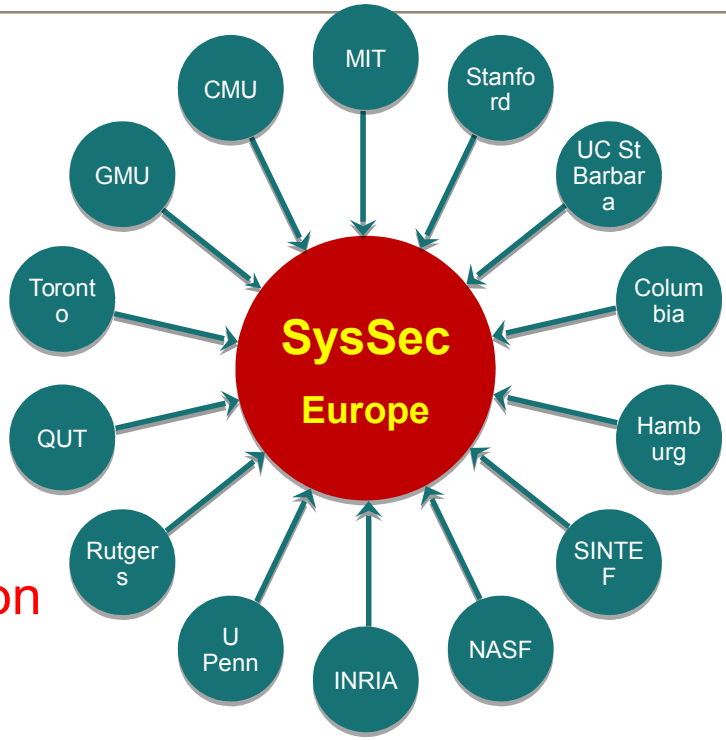


SysSec Aim and Objectives (I)

- Create an active, vibrant, and collaborating **community of Researchers**
- SysSec aims
  - to create a **sense of ``community''** among those researchers,
  - to **mobilize** this community,
  - to **consolidate** its efforts,
  - to **expand their collaboration** internationally, and
  - become **the single point of reference** for Systems Security research in Europe.

Community building efforts

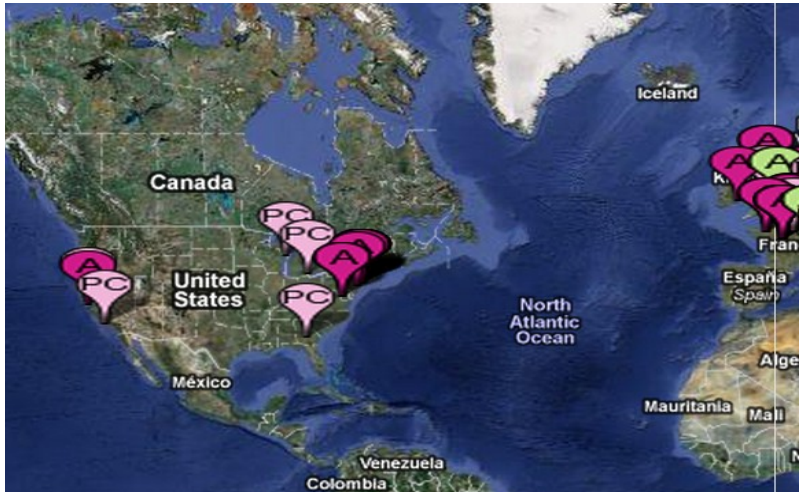
- Associated partners:
  - The broader Community of SysSec
- Selection:
  - "Call for Associated Partners"
    - Selection by the project's "Evaluation Committee"
- Financial Support for Associated Partners:
  - Cover trips to visit core partners
  - Provide scholarships for research collaboration with core partners



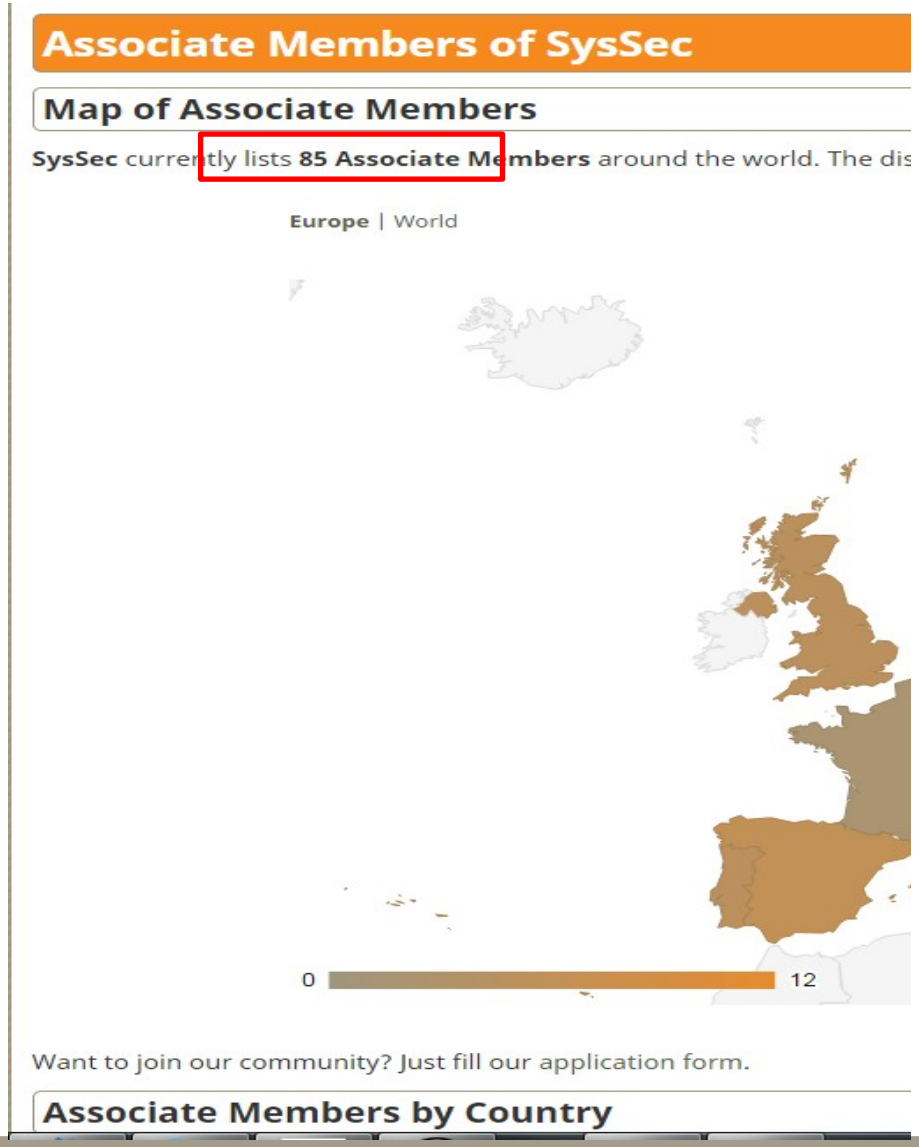
- Budget:
  - 100.000 euros for short-term scholarships
  - 100.000 euros for travel support

First 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



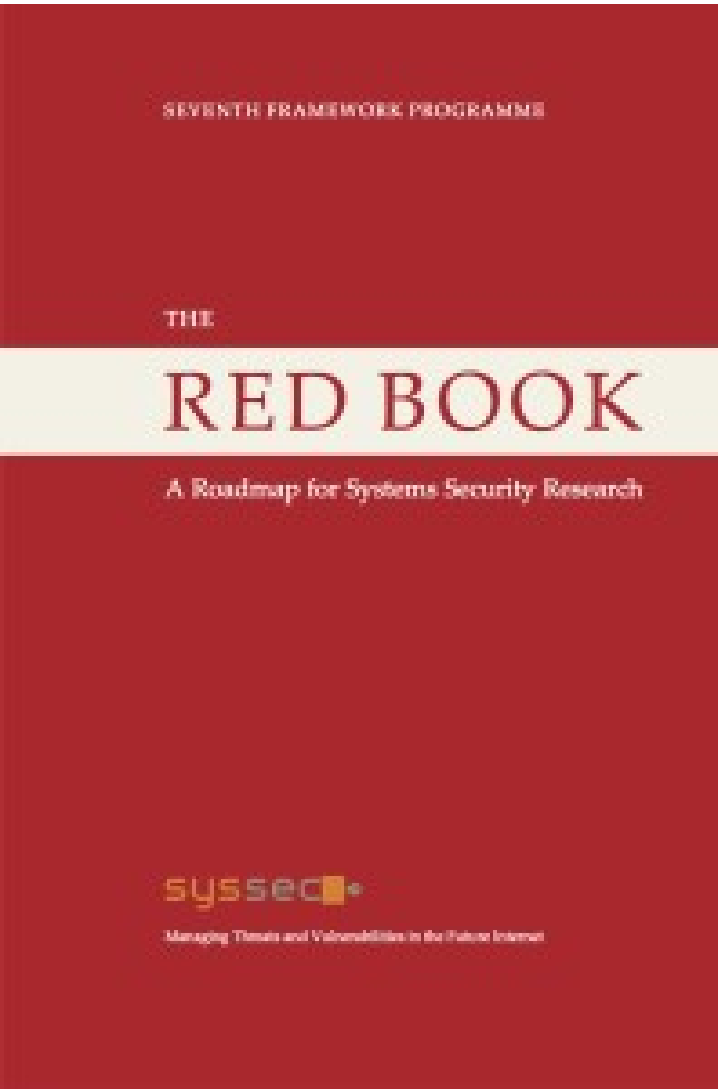
Associated Partners



SysSec Aim and Objectives (II)

- 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.

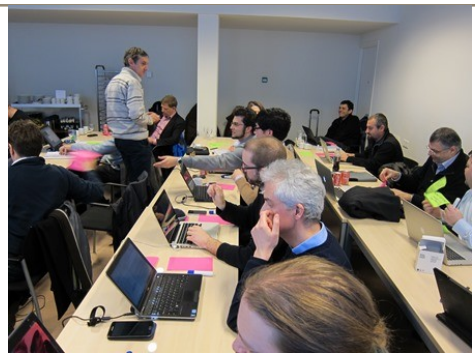
The Red Book



- Please download it!
- www.red-book.eu

The making of the Red Book

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



SysSec Aim and Objectives (III)

- 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,
- 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.

Educational results

Courses designed/redesigned	**11**
Participating Universities	**31**
Scholarships awarded	**22**
Graduated Ph.Ds	**10**
Graduated Masters	**40**

Summer schools

syssec

About ▾ Community ▾ Events ▾ Scholarships ▾ Publications Publicity

2nd SysSec Summer School

SysSec organises a School on **Mobile Malware (Theory and Practice)**. It will be held on **September 25-26, 2014** in Amsterdam. Visit our related page for more information.

Registration is now open!

SysSec organises a School on **System Security and m reverse engineering with a special focus on infrastructure protection**. It will be held on October 2012 in Amsterdam. Read our related page for more inform

Update (11/9/2012): Registration for the SysSec Summer School is now closed! The interest school has been very significant and **all the available places have been filled**. People that have registered their interest will be sent out to either confirm their participation, or if they registe late, inform them that they are in a queue pending cancelations of students.

Summer schools

10K students challenge

- Educate 10,000 students in buffer overflows

Who joined the 10K Challenge?

- More than 50 University Courses
- Most European Member States
- USA, Canada

How?

- First: general idea
  - How does a computer work?
  - Function calls, stack, etc.
  - Stylized buffer overflow
  - ➔ Toy processor
- Next: for real
  - real code and real CPU
  - Real buffer overflows
- Finally: counter-measures
  - Canaries
  - DEP
  - ASLR

Educational material

- General Introduction [pptx][pdf][YouTu
- Part I - Basic Buffer Overflows (Everyone)
- Part II - Real Buffer Overflows (Computer Scientists) [pptx][pdf][YouTube][Questions]
- Part III - Countermeasures (Students in Security Courses) [pptx][pdf][YouTube][Questions]
- Notes about compiling the code examples in the slides [pdf]

Instructors will receive the answers to the questions above during the registration process.

Also, visit our common curriculum **here** to find educational material on other aspects of system secu

SysSec Aim and Objectives (IV)

- 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 to play a major role in the area.
- 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.

Publications

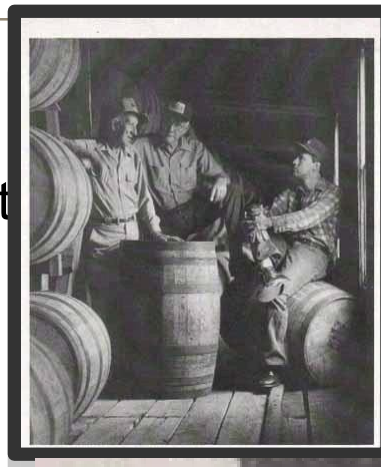
- Extensive publication track
- 153 peer-reviewed papers
- 20% in top tier venues
- 114 additional presentations and seminars

Where are our students now?

- Google, Facebook, Microsoft, Ericsson Research, Ericsson, Secure Network Srl, Anaplan, Acquire, CEFRIEL, Amadeus, Gaisler Aeroflex, IBM Research, TrendMicro, LastLine, etc.

Key insight: appropriate duration

- Research feedback loop is 4 (plus) -years long:
  - Predict threats–> address them –> seen in the wild –> get feedback
  - Tried to have at least one entire loop (i.e. seen in the wild predicted threats) before the end of the project
- Education loop is 4 (plus) years-long
  - Get associated-partners (users) on board: one-two years
  - Design of the curriculum: one year
  - Implementation/evaluation of the courses: two years+
- Consolidate the Systems Security Research Community in Europe (1-2 years) and establish the framework for a joint work programme (1 year) + implementation (1+ years)



What's next?

- Give back
  - Give back our expertise to the research community
  - Give back our expertise to the innovation community
  - Give back our expertise to policy makers

Give back to Research

- We put Europe in the map of Systems Security and Privacy
  - We need to strengthen our position
  - Train more researchers
  - Staff more Universities
  - Make Europe not a player but a leader in the area
    - We have the know-how
    - We have the expertise
    - We have the policy support (esp. for privacy)

Give back to policy

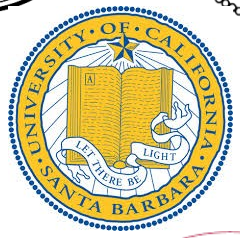
- Give back to policy makers
- How can we help Security Research Policy?
- Contribute
  - to roadmaps
  - to policy decisions
  - To prioritize alternatives
  - Map the future

Give back to innovation

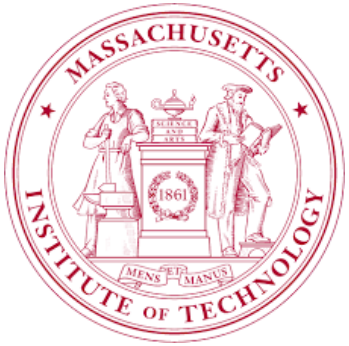
- Help innovators
- Identify gaps
- Offer solutions
- Train innovators
- We have the know how
- We have the necessary culture
- We have the youthful minds

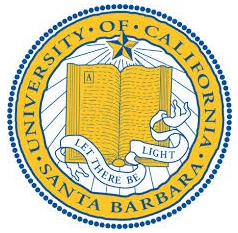
Next step in education and training

- We were excited by the success of mobility grants and joint research
- We built the project PROTASIS
- A Marie Curie RISE project
- Mobility funds for young researchers



RISE: intersectoral and international





Conclusions

- What we achieved
  - Put EU “back on the map” in cybersecurity research
  - Trained excellent professionals and researchers
  - Gave back to policy and public sector

Our next objective:

Create opportunities for young researchers and talented leaders to connect with the world, but remain rooted in the European Union

Thank you!

- Questions and feedback
  - Now!
  - Via e-mail stefano.zanero@polimi.it
  - Via twitter :-) @raistolo