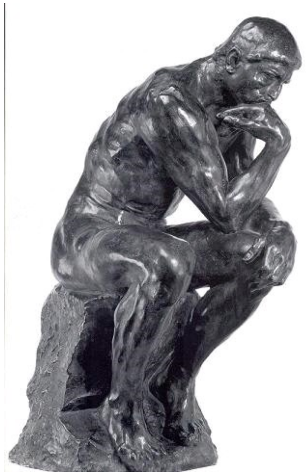
Industrial impact of a NoE: the approach of SysSec

Stefano Zanero
Politecnico di Milano

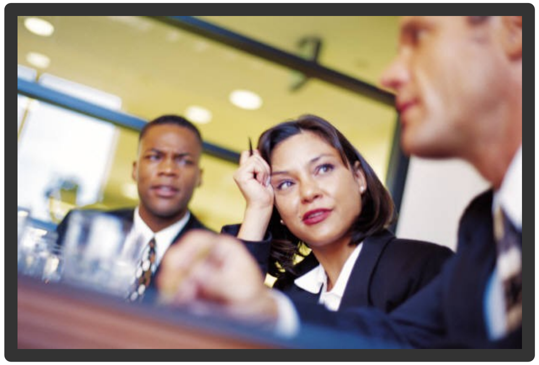


SysSec: addressing change

- The technology is changing
- The society is changing
- The attackers are changing

SysSec: the work plan

- Created three working groups of experts in
  - Malware and Fraud
  - Smart Environments
  - Cyberattacks
- Brainstorm on emerging Threat
- Created a list of research areas



Industrial engagement?!

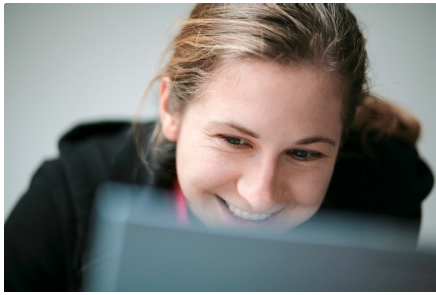
- NoEs do not have industrial partners in FP7
- However, the PO and the reviewer like to see industrial exploitation
- In fact, many of the research areas we identified have evident industrial fallouts!

Identified Research Areas

- Privacy
- Targeted attacks
- Mobility
- Usable Security
- New and **Emerging technologies**

Privacy

- Help users gain control of their data (business advantage opportunity)
- Detect attempts
  - to correlate data
  - to de-anonymize user accounts by correlation
  - Consumer product(s) opportunity



Targeted Attacks

- Collect and analyze data
  - Of targeted attacks
- Create data repositories
  - Exchange Data among international partners
- New Defense approaches
- Understand the financial motives and structures behind these attacks
- Prevention at the ISP level

Mobility

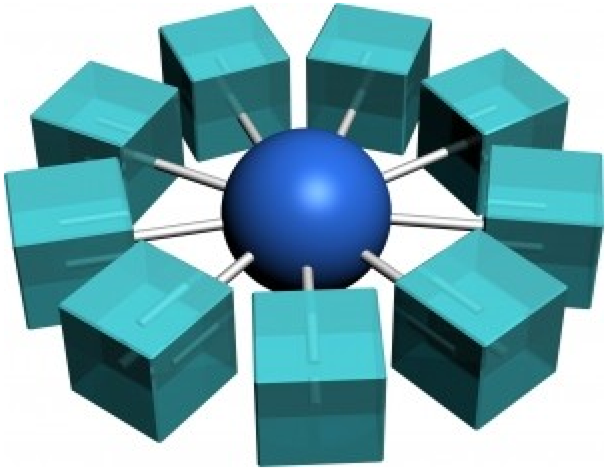
- Mobile phones
- New tools
  - To be deployed on smart phones
  - for attack detection/prevention

Usable Security

- Focus on the weakest link
  - i.e. human beings
- Interdisciplinary efforts
  - Engineering, system security, psychology, etc.

New and Emerging Technologies

- Cloud Computing
- Social Networks
- Smart meters
- **Smart cars**
- SCADA networks



Example of industrial fallout

- Polimi worked on security of a smart vehicle
- We created a framework for securing vehicle/smartphone interactions
- (submitted for publication @ ESCAR)
- This was enabled by a SysSec mobility grant
- Piaggio (the vehicle manufacturer) is following up for industrial implementation

Industrial engagement best practices

- Created an industrial advisory board (IAB)
  - Get feedback on our deliverables
  - Get input for the roadmap
  - Get input on the curriculum
- Invite industrial experts to our conferences and schools
- Interact with the industrial contacts of partners
- We are here today to hear other best practices from other projects

How can you get involved?

- Comment on our Roadmap
- Join our mailing list
- Attend our School
  - Oct. 11-12, 2012 in Amsterdam
  - Topic: security of critical systems
- Contribute to our curriculum
  - On systems security
- Become an associated member