Future Research on Systems Security

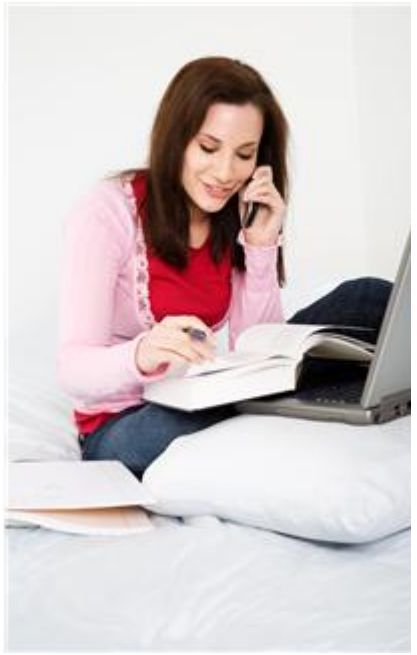
Evangelos Markatos
the SysSec Project

A world of change

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

The technology is changing

- Mobile phones
- Smart environments
  - Smart power meters,
  - Smart homes, appliances
  - Smart cars, city cars
- Disappearing computers



Things Babies Born in 2011 Will Never Know

- The separation of work and home
- Wires
- Hiding
  - Can you hide in an on-line world?
  - Privacy?

Source: http://finance.yahoo.com/family-home/article/111745/things-babies-born-in-2011-will-never-know?mod=family-kids_parents

The society is changing

- New ways of interaction: social networks
  - Who are your friends?
- Always "available" culture:
  - People are accessible 24/7 for work and fun
  - Important decisions are taken "on the go" from a mobile phone
- We depend on technology

The attackers are changing

"… 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 European Commission

What did we do?

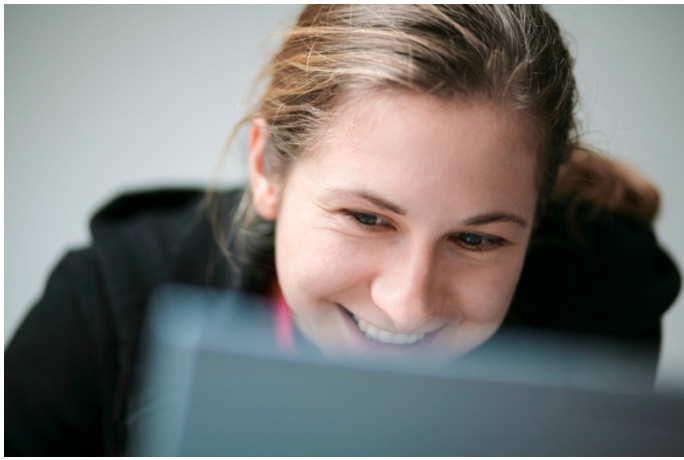
- Created three working groups of experts in
  - Malware and Fraud
  - Smart Environments
  - Cyberattacks
- Brainstorm on Emerging Threats
- Created a list
  - of research areas
- Got feedback from the Industrial Advisory Board

This is what they came up with

Malware and Fraud

Malware and Fraud

- Malicious Hardware
  - Compromised routers, processors,
- Attacks Against the Cloud
- Advanced Malware
  - Propagating in social networks
- Mobile Malware
  - Malware for mobile devices (e.g. phones)
- Information Risks – Data gathered
  - Government-collected data
  - Data collected by service providers
- Targeted Attacks



Smart Environments

- Accessibility
  - Routers, ah hoc networks, smart meters, etc.
- System Complexity - maintainability
  - Too many sensors/computers in a smart home
  - Are all my devices up-to-date?
- Attacks against the non-ICT component
  - False sensor data
    - Heat, radiation, pressure, etc.

Cyber attacks

Cyber attacks

- Web Services and Applications
- Privacy
  - Target private data e.g. in social networks
- Critical Infrastructures
  - Power supply?
  - Emergency services? 911 (US) 112 (EU)

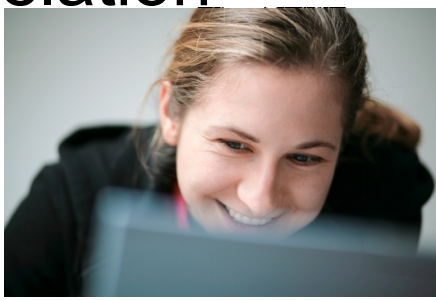
- Smart, Mobile and Ubiquitous Appliances
- Insiders
- Network Core Attacks

Suggested Research Areas

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

Privacy

- Help users gain control of their data
- Protect them from disclosing their data
  - Do I really need to send all these tracking cookies around?
- Detect attempts
  - to correlate data
  - to de-anonymize user accounts by correlation

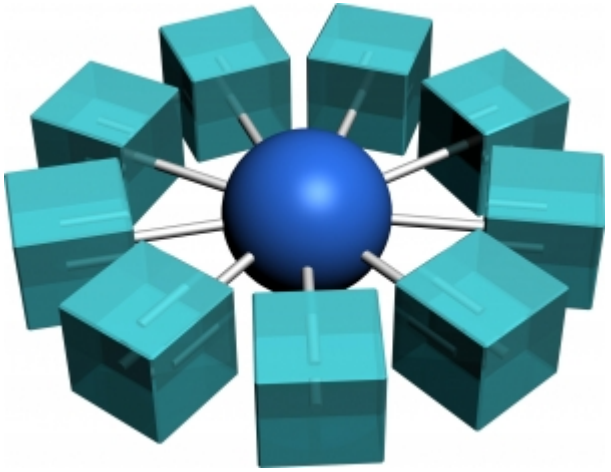


Targeted Attacks

- 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

New and Emerging Technologies

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



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.

Summary

- Everything is changing
  - Technology, society, attackers
- We need to understand new attacks
- Focus on
  - Privacy
  - Targeted attacks
  - New and Emerging technologies
  - Mobility
  - Usable Security

Future Research on Systems Security

Evangelos Markatos
the SysSec Project