Future and Emerging Threats in Information and Communication Technology Infrastructures

Sotiris Ioannidis
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece
Goals

• The future is hard to predict…
  – Worms
• … but we have had success stories
  – RFID
• The FORWARD Project is a coordination action
  – Bring together academics, industry, and policy makers who are interested in emerging threats in ICT
  – Discuss future threats
  – Develop realistic scenarios
The Working Groups

- Smart Environments
- Malware and Fraud
- Critical Systems
Threats

- Underground economy
- New vectors to reach victims
- Hardware malware/Malicious hardware
- Advanced botnets
- Attacks against the core Internet protocols and services
- Privacy and trust abuses in online communities
- Targeted attacks, spear phishing
- Naming and fast flux networks
- IPv6 and direct reachability
- Mobile device malware
- Attacks against financial sector
- Attacks against virtualization
Threats cont.

- Smartphones into zombies
- Spyware in the bedroom
- False sensor data
- Maintainability and verifiability
- RFID
- Attacks against office equipment
- Attacks to home automation
- Aviation security
- Multicore threats
- Threats due to scale
- Wireless plane attacks
Conclusions

• Factors driving emerging and future threats
  – New technologies
    • Wireless, device miniaturization, etc.
  – New applications
    • E-government, E-commerce, etc.
  – New social dynamics
    • User connectivity, social networks, etc.
• www.ict-forward.eu