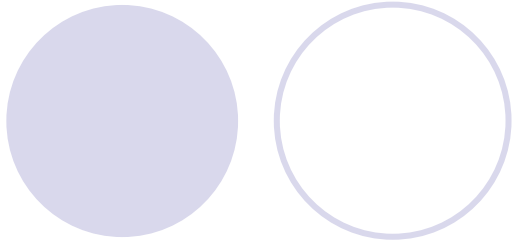


# Security challenges in the future internet

Sokratis K. Katsikas

Member, Hellenic Authority for Information and  
Communication Security & Privacy  
Professor, University of Piraeus

[ska@unipi.gr](mailto:ska@unipi.gr)



- Will not be just an evolution of what we see today: no more a network that reaches out to terminals, but objects, including terminals, having their own connectivity halo, will be able to connect to other such halos.
- Will be the sum of it all, but this does not mean ubiquitous use of IP (sensor networks, body area networks, vehicular networks).
- Will comprise objects with embedded communication capabilities, forming a communication network able in turn to connect to other communication networks.

# The Internet of the future...

- It will be a seamless fabric of classic networks and networked objects.
- Therefore, radically new approaches are needed: new architectures, new interfaces, new ways of managing data, new ways of integrating all the different internet entities (devices, sensors, services, things, people)

# The Internet of the future...

- Will need to be architected differently
  - Seamless mobility; personal information and content available anywhere, anytime; context-aware environments.
- Will bring new ways to create value in the web-based service economy
  - Design your car
  - Merging of the physical and the digital world.

# The Internet of the future...

- Will increasingly include Things.
  - Talk to your washing machine
  - Smart items
- Will bring about new challenges for regulation and ethics.
  - Create your personal memory space on your mobile
  - Regulation evolves at a much slower pace than technology
  - Privacy and security must be built into every service since the design phase

# Security challenges...

- The architecture

- Need to ensure that a number of diverse technical components with increasing complexity are flexible and secure.

- The preservation of societal values

- New threats, new risks
- Privacy, transparency, accountability, open and fair operation of the future internet, competitiveness of the e-services market

# Security challenges...

- Security that does not get in the way
  - Security should not impede efficiency and user acceptance
  - Usability, economics, awareness, education, literacy
- Aligning value protection with future internet models
  - Connectionless vs connection oriented vs “value-based” model of operation

# The future trusted internet

- The importance of trust
- Protection of user credentials and privacy-friendly ID management
- Protection of nodes and devices against misconfiguration and malware
- Trust in communicating as well as in processing

# Sources



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ  
ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Future Internet 2020: Visions of an industry expert group, May 2009, DG Information Society and Media, European Commission. <http://www.future-internet.eu/>
- NESSI TSD WG Position Paper on Security Challenges in Future Internet <http://www.think-trust.eu/>