
NIS Platform: Aol „Trustworthy (Hyperconnected) Infrastructures“

Steffen Wendzel (Fraunhofer) and Piero Corte (Engineering)

steffen.wendzel@fkie.fraunhofer.de



Overview on current state

- Currently 18 participants registered for Aol on Trustworthy (Hyperconnected) Infrastructures
 - 12 industry
 - 6 academia

Overview on current state

- Aol's vision (core idea):

- *“Participants see future infrastructure processes and resources as **adaptive, de-central, collaborative and efficiently controlled**. Most (especially critical) infrastructure must be **reliable, predictable and always available** [...]; it should be capable to **react to cyber threats in real time**. [...] A key aspect [...] will be the surrounding of citizens by network devices in the context of ubiquitous computing. [...] **Future cities for European citizens depend on (C)I and compete for human resources as each city must be optimized to use its (C)I in order to motivate skilled people to stay in the city/to move to the city.**”*

Overview on current state

- Major topics identified:
 - ICT infrastructure, transportation infrastructure, smart grids, smart buildings, smart cities, industrial control systems, automotive/electrical vehicle charging
 - Links to exiting research projects (especially exiting FP7 projects)

Major challenges identified (selection)

- Migration of legacy systems / protocols / standards
 - Introducing security features into old systems is challenging
- Keeping infrastructure secure if it “grows” and becomes inter-connected with other infrastructure
- Handling the rapid growth of attacks as well as novel, sophisticated attacks
 - in less time
- User-tailored security solutions

Exemplary Outlook

■ Smart Building Security

- Considered part of the “legacy” problem
- Very old communication protocols, bad security
- Requires solution capable to introduce security without breaking the building automation system
- One approach: traffic normalization

■ Steganographic Malware

- Future botnets and malware will hide traffic in much more sophisticated manner
- It will take years to create suitable countermeasures

Dr. Steffen Wendzel
steffen.wendzel@fkie.fraunhofer.de
Cyber Defense Research Group
Fraunhofer FKIE
DE-Bonn