Internet 2013 Panel

How Much Safe Cooperation Can Internet Handle Now

Panelists

Danco Davcev, University Ss Cyril, Macedonia
Yasuhiko Watanabe, Ryukoku University, Japan
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Elena Troubitsyna, Abo Akademi University, Finland

Network Design
Research Center

Cooperation & Security tension

Cooperative actions and threats

- File sharing – virus spreading
- Code sharing – bug spreading
- Idea exchange – IP leakage and contamination
- Remote communication – Information leakage

Evolution of Cooperative Work

Non real time

- Email based cooperation
  - Account spoofing
- Internet Relay Chat rooms
  - Anonymity and impersonation
- Web Services
  - Secure server access

Real time

- Video conferencing
  - Session eavesdropping
- Messengers
  - Conversation leakage

Cooperation at Workplace

Cooperation at Academia and Industry workplaces

- Malicious software/virus infection
- Telecommuting/VPNs
- Bring your own devices (BYOD)
  - Data Protection
  - Corporate mailbox secure access and isolation
  - End of life issues

Future of Safe Cooperation

Academic and Industry cooperative work - security issues

- Are current security procedures and protocols adequate?
  - Encryption, Authentication, Access Control, VPNs
- What new security technologies could foster collaborative work over the internet?
- How will emerging internet technologies/collaborative applications impact security schemes?
  - Cloud computing
  - Internet of Things

Openness challenge to resilience

Elena Troubitsyna
Åbo Akademi University, Finland

Resilience of open collaborative environments

- Resilience - the ability of a system to deliver services that can be justifiably trusted despite changes

- It encompasses the system aptitude to autonomously adapt to evolving requirements, operating environment changes and/or failures

- Collaborative working environments now replace traditional office
  - Security threats, volatile architecture, inherent unreliability, large variety of failure modes

Challenges in engineering resilient collaborative environments

- Complexity of the cyber environment
  - Coping against unknown

- We need scalable resilience-explicit engineering techniques providing continuum between the design stage and run-time

- Highly dynamic nature of future collaborative systems
- Need to support compositionality
  - Some attributes are not compositional
  - Reasoning about emerging properties

- Emphasis on run-time verification
  - On-line extraction of models
  - Compact representations

Monitoring: safe vs harmful

- Monitoring to learn patterns of use and interactions
  - Help to optimise performance, improve interface, diagnose and remove faults

- Improper use of data by monitoring party
  - How to achieve accountability?
  - Monitoring security contracts?
- Data in Cloud: who owns the data?

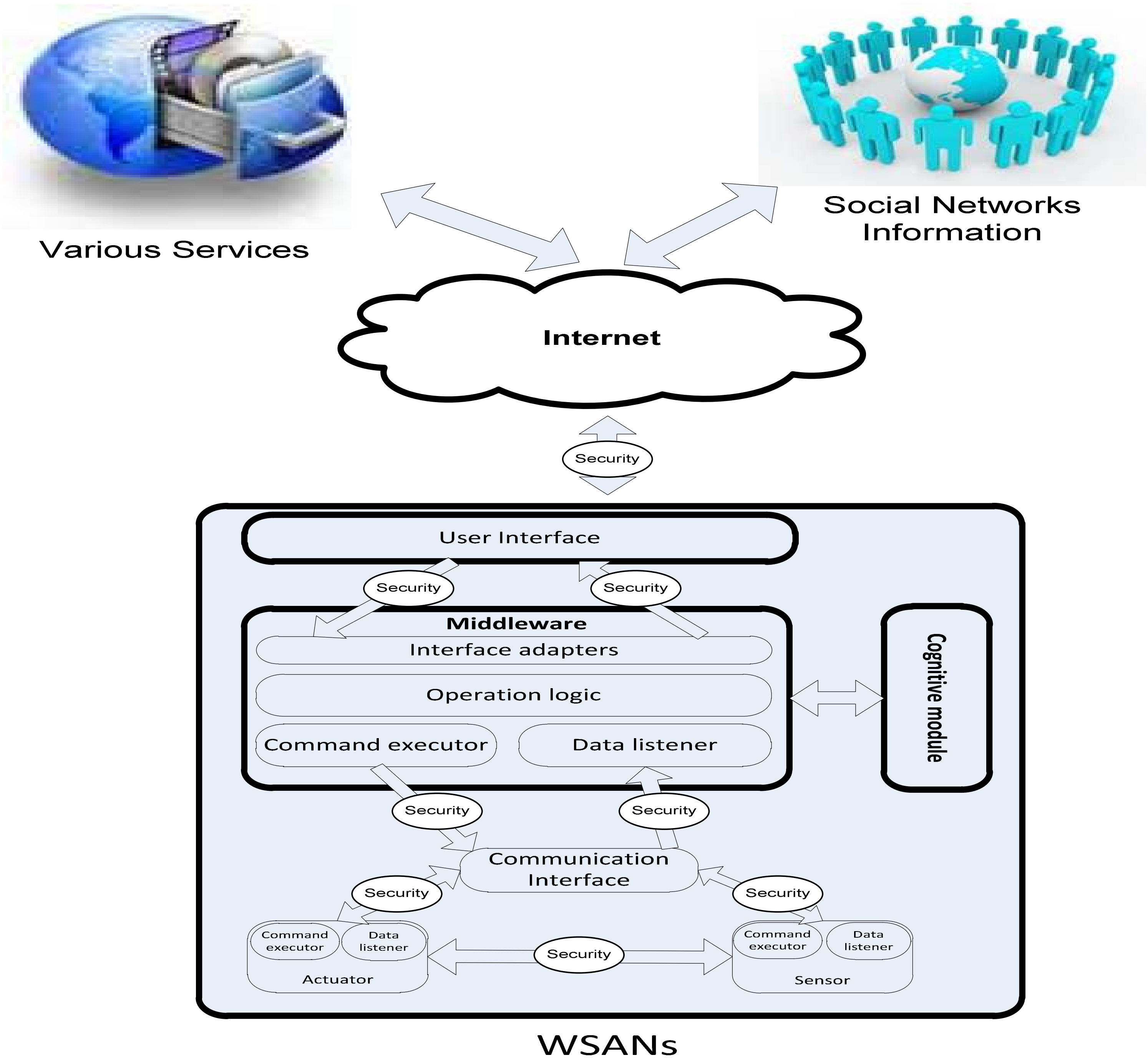
Cyber security in the Internet of Things (IoT)

Professor Danco Davcev

Computer Science and Engineering

Challenges for IoT security architecture

- Future IoT is the fusion of the physical, cyber and social world.
- The nervous system structure in the human body and social organizations are good examples for designing IoT security architecture.
- Three layers architecture :
  - sensor actuator networks (SANET)
  - global network and
  - application layer.


Various Services
Social Networks Information
Internet
Security
User Interface
Security
Security
Middleware
Interface adapters
Operation logic
Command executor
Data listener
Cognitive module
Security
Security
Communication Interface
Security
Security
Command executor
Data listener
Actuator
Security
Command executor
Data listener
Sensor
WSANs

Security

- Securing WSAN is challenging because these networks rely on an open medium of communication, cooperative by nature and hence lack of centralized security enforcement points e.g., routers, from which preventive strategies are launched.
- Thus, traditional ways of securing networks relying on e.g., firewall, should be enriched with reactive mechanisms, e.g., **intrusion detection system**.
- **A distributed and cooperative intrusion detection system** based on **cognitive analysis** should be developed.

IARIA INTERNET 2013

How much safe cooperation can Internet handle now

yasuhiko watanabe

ryukoku university

Our activities in pseudonymous space

- Communication

  SNS, micro blogs, Q&A, etc.

- Business

  crowd sourcing, auction, etc.

Study and understand

- What
- How
- Why

we do

in pseudonymous spaces

We need big data of pseudonymous users' behaviors

- Yahoo! Chiebukuro (Japanese Yahoo!answers)
  - – Questions (16 million submissions)
  - – Answers (50 million submissions)
- Rakuten data
  - – Product data (50 million items)
  - – Review data (20 million items)