NexTech 2023

Theme
Security Challenges in Cyber-Systems

PANEL: CPS Security

PORTO
September 2023

CPS Design

- Ubiquitous, both CPSs themselves and connectivity in general
- Careful design according to standards, e.g., medical-grade
- Design time security possible
- However, often not possible: time/money constraints: “in IoT, the ‘S’ stands for security”

Human Factor

- No CPS possible without human factor.
- Cons: Humans manipulatabe, even despite our best intentions
- Security factor ≠ level of expertise
- Pros: Human-machine teaming a possible venue
- Decision support and increase of situational awareness goal

ML/DL/DRL

- The new old kid on the block: Much hype, but also new possibilities
- Well-known usages include heuristics
- “Post-modern” DRL agent architectures probe for weaknesses, increase situational awareness, even provide resilient operation (“assistant”)

CONTRIBUTORS

Moderator

Dr. Eric MSP Veith, Carl von Ossietzky University Oldenburg, Germany

Panelists

Dr. Rainer Falk, Siemens AG Technology, Germany

Prof. Dr. Joshua Sipper, US Air Force Air Command and Staff College, USA

Dr. Kate-Riin Kont, Estonian Academy of Security Sciences, Estonia

Prof. Dr. Anders Fongen, Norwegian Defence University College, Norge

Prof. Dr. Dirceu Cavendish, Kyushu Institute of Technology/UCLA, Japan/USA

Panelist Position

Porto
Sept 2023

Dr. Rainer Falk
Siemens AG

- **Cybersecurity for Industrial Systems**
  - Industrial systems need a security design that address the relevant security objectives and respect side conditions for the specific environment (e.g., lifetime, real-time, functional safety, usability).
  - The industrial security standard IEC62443 is applied in different verticals. The responsibilities of the different roles (system operator, integrator, component manufacturer) are distinguished.
- **Cybersecurity Demand**
  - Cybersecurity increasingly driven by regulatory requirements
  - Industrial Metaverse and digital twins – combining the real and the digital worlds
  - Cyber resilience to keep cyber systems operational under attack
  - Usability of security, security by default, security by design, zero trust security
  - Upcoming technologies, e.g., PQ crypto, AI/ML, AR/VR, IoT, TSN, 5G/6G, edge computing, virtualization

Panelist Position

Porto
Sept 2023

Josh Sipper
ACSC

- **Cyber Systems: Numerous Types and Attack Surfaces**
  - Cloud Platforms: Virtualized machines and data
  - Internet of Things: Billions of potentially vulnerable devices
  - Industrial Internet of Things (Industry 4.0): Billions of critical infrastructure devices
  - Military Internet of Things: Connected devices, weapons, radars, MANET, etc.
  - Wireless Networks: 5G and future generations transmitting massive amounts of data
  - Space Networks: Satellite on-board processing, ground-station vulnerabilities, ViaSat, etc.

- **Securing Cyber Systems: Recommendations and Mitigations**
  - Continued boundary defense and VPNs
  - ZTNA
  - AI/ML heuristics
  - Human/Machine teaming
  - Decision-support systems
  - Quantum random-number generation for encryption
  - Future quantum encryption through entanglement/superposition

Panelist Position

Porto
Sept 2023

- **Human factor in cybersecurity**
  - The ability to exploit human nature with relative ease has created a situation where many cyber-attacks focus on human weaknesses. It is necessary to increase the awareness of organisations and their employees about information security and to promote their ability to deal with unsafe behaviour related to cybersecurity.
  - In order to reduce the risks related to the human factor of information and cybersecurity, several reliable scales and methodologies have been developed to measure risky attitudes and of the organisation.
  - **Cyber resilience, management behaviour and individual personality traits**
  - While cybersecurity is highly valued, it does not mean a high level of expertise. This means that key areas that would increase the cyber security of organisations are often not invested in. This leads to a reactive approach to cyber incidents rather than a proactive approach to mitigating cyber risk.
  - Employees tend to underestimate their likelihood of becoming a victim of cybercrime and that it is organisational, environmental and behavioural factors that influence the extent to which employees adhere to cyber security rules or good practices. An employee's commitment to the organisation is also likely to play a role in his or her security behaviour and positively influence the employee's intentions to comply with the security policy.

Dr. Kate-Riin Kont
Estonian Academy of Security Sciences

Panelist Position

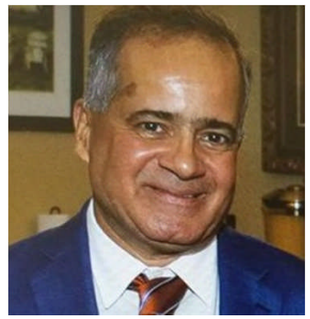
Porto
Sept 2023

Dr.Anders Fongen, Norwegian Defence University college

- **Design Time Security in IoT**
  Short time to market, Lack of expertise, Lowest bidder: No time and no skills for design-time security
  Secret design and protocols: No independent scrutiny of implementation
  The risk is that severe vulnerabilities remain unnoticed in IoT equipment for years (ref. Heartbleed)
- **Observations of users – distribution and usage**
  How is trading of users' observations taking place: Possible fusion of user data allows deeply private psychological traits to be exploited for marketing (not bad) and manipulations (social engineering, hybrid warfare) ref: Cambridge Analytica
  Can applications be restricted by software-based restrictions? Probably no.
  Can the public be made aware of these risks? Some, maybe
  May AI play a role as a "good guy" on these problems

Panelist Position

Porto
Sept 2023



Dirceu Cavendish
Kyushu Institute
of Technology

- **Security/Privacy in Medical Systems**
  - Complex Networked Medical Systems increases security threats
  - Diverse computing technologies multiply security threats

- **Medical Systems Cybersecurity Requirements**
  - Security as a design goal, not afterthought – medical grade security definition
  - Revamping of Medical Machines OSs
  - Secure Hospital Management Systems
  - Medical grade secure Cloud Computing
  - Medical grade secure smartphone applications
  - Medical grade secure embedded devices: sensors; actuators

Output highlights