CHIST-ERA Projects Seminar
Cross Topics
Resilient Trustworthy Cyber-Physical Systems (RTCPS)

Speaker
Awais Rashid
(Lancaster University, UK)

Brussels, March 22-23, 2017
FBI: Hacker claimed to have taken over flight's engine controls

By Evan Perez, CNN
Updated 0219 GMT (0919 HKT) May 19, 2015
Four projects in RTCPS

- COPES: Consumer-centric Privacy in Smart Energy Grids
- DYPOSIT: Dynamic Policies for Shared Cyber-Physical Infrastructures under Attack
- I-DRESS: Assistive Interactive Robotic System for Support in Dressing
- SECODE: Secure Codes to Thwart Cyber-physical Attacks
Not an anarcho-syndicalist collective!

COPES

Information Security

Personal Information

Change Management

DYPOSIT

SECODE

I-DRESS
Energy consumption profile reveals personal information! Privacy risk!!!

(Copied) EU General Data Protection Regulation strongly protects private life
• Potential show stopper

COPES approach: Manipulate actual energy consumption profile using energy storage & alternative sources
Major Results: SM Privacy Measures and Privacy Enhancing Technology

- Design of several energy flow control algorithms considering
  - Different privacy measures (past focus)
  - Utility (e.g. energy-cost) – privacy trade-off (future focus)

- Privacy-by-design!

- 7 conference & 3 journal papers published/submitted
- Outreach to several agencies, companies & events + webpage
- 2 expert advisory roles

- 3 granted *follow-up research projects* on impact of energy storage technology
- Proof-of-concept experiments in KTH Live-In-Lab planned
Security policies as living, evolving, objects that play a central role in reasoning about the security state of such a CPS and responding to unfolding attacks.
DYPOSIT: Key Results to Date

**Attack Analysis**
- Ethnography-style study of an actual cyber-physical system
- Testbed analysis and implementation of a range of attacks

**Dynamic Policy Models**
- Model for dynamic change in an ICS configuration
- Reason about policies using refinement and composition operators

**Attack Detection**
- SimaticScan: A specialised vulnerability scanner
- SENAMI: Selective, non-invasive, active monitoring for intrusion detection

**Platforms**
- CerberOS operating system for IoT devices
- Secure application loading and strong isolation, contractually limited access to resources.

- 8 scientific publications
- International workshop on topic
- 4 keynotes and invited talks
- Additional testbed

- Software prototypes
  - CerberOS
  - SimaticScan
  - SENAMI
I-DRESS: Robotic Dressing Assistance

Aims of I-DRESS project

- Algorithms for pose and garment tracking
- Recognising user's attention and intentions
- Learning from Demonstration algorithms
- Hazard analysis for safe robot operation
- Multimodal user interface for safe physical interaction
- To integrate on a commercial robotic platform.
I-DRESS Achievements

- Pose and gesture detection algorithms
- Human-Human-Interaction testing
- Discrimination between garments using force
- Learning by demonstration (video)
To use Codes to thwart Cyber-physical Attacks:

- Specify and design error correction codes suitable for an efficient protection of sensitive information in the context of Internet of Things (IoT) and connected objects.
- The protection based on codes is to avoid/mitigate:
  - Passive attacks,
  - Active attacks
- Study and Use of LCD (Linear Complementary Codes) or LCP (Linear Complementary Pairs) codes, well suited for masking protection
Enhance the Code Theory:
- Design of "Linear Complementary Dual" LCD codes

Assess the security level based on Code:
- What are the Security parameters against Physical attacks?

Implement a Cyber-physical protected platform:
- Based on modified LLVM
- Automatic insertion of protection based on codes
Estimated 50bn connected devices!
Estimated 35 zeta-bytes \((35 \times 10^{21})\) of digital records!
And hyper-connectivity!
Future Research Direction for RTCPS

- **Digitalisation – Security and Privacy Ergonomics by Design**
  - Gap between person’s understanding and what goes on in the system
  - Human in-the-loop
    - Automation vs. agent interaction
    - Leveraging the human as a resource
  - System and software architectures
  - Skills gap
  - Socially engaged cyber-physical systems
    - Security economics
    - Privacy dynamics

- **Developing as a discipline and/or shaping the various disciplines**
Challenges and Opportunities

- Privacy – little incentive for industry? (participatory data economy)
- Security – economic incentives for industry, finally! (critical infrastructure and systems)

- H2020 – Secure Societies
  - Leverage existing security research
  - What is needed is more foundational focus (lower TRL)
    - National and European funding programmes
    - Need multiple competencies across Europe (particular for smaller EU countries)
Security and Privacy Ergonomics

Digitalisation

Expertise

The cradle of ergonomics

Automation

Security and Privacy
Questions ?