Security Applications and Challenges in Networked Embedded Systems

Dr Dirk Pesch
Head of Centre
Nimbus Centre for Embedded Systems Research
Cork Institute of technology, Ireland
Cork Institute of Technology

- Ireland’s second largest Institute of Technology
- Located in Ireland’s second largest city, Cork, in the South of Ireland
- CIT offers Bachelor, Masters and PhD degrees in Science, Engineering, Business, Art and Music
- Some 12000 students and approx. 1000 academic & research staff
The NIMBUS Centre

- Focus on networked systems research
- Application Space – Smart Energy Management, Security and Safety, Vehicular/Traffic, Health/Hygiene
- 60+ researchers focusing on fundamental and applied research

- Three research groups
  - Adaptive Wireless Systems
    - Wireless Network Design
    - Algorithms & Protocols
    - Real-time Localisation & Tracking
  - Smart Systems Integration
    - Sensor Device Integration,
    - Miniaturisation and Embedding of Electronics
    - Integral Sensing Networks
  - TEC Centre industry R&D group
Nimbus Centre Research

• **Application Focus Areas**

  • **Smart Energy Management Systems**
    • Wireless sensor/actuator networks for building management
    • Design tools for wireless network planning in indoor environments
  
  • **Infrastructure and Personalised Safety/Security Systems**
    • Sensor fusion for localisation of
      • people, vehicles, objects in airport environments
    • On touch authentication systems
  
  • **Smart User Interfaces**
    • Embedding of sensor devices into materials and objects
    • Real-time Interactive Sensor Information Visualization with Multi-touch Technology
Networked Embedded Building Management Systems

• Increasing instrumentation of buildings with wired/wireless sensing and control technologies
  • Sensing of ambient parameters, e.g. temperature, light, humidity, CO2, occupancy etc. for energy management and user comfort
  • Access control system used for security

• Integration of individual BMS
  • Sharing of information between energy management and access control systems
    • Enhance occupancy detection for better energy management
    • Increase systems reliability

• Increasing use of wireless technologies
  • Several standards with weak security
Occupancy Detection in Buildings

• **Use of sensor data to detect occupancy**
  - Typically PIR sensors

• **Organisations want more detail for building control – energy & comfort**
  - Is a person in a particular room/location?
    - Aim is to use largely existing sensors – PIR, access control but also information from user’s computers, temperature, CO2

• Occupancy detection has potential to create security vulnerabilities
  - Identity of users
  - Are users in a particular location allows inference such as is a house occupied
  - Protection and anonymity of information
MapUme is an opportunistic localisation system which fuses location related sensor information that is readily available to localise people and objects.
LocON - Platform for Safety and Security Enhancement
for large critical infrastructures like airports

Key components:
- **Sensor and actuators networks** – (Loc. + surveillance + environment system)
- **Context awareness** – (moving objects and unexpected events)
- **Advanced real-time processing** – for collision avoidance and navigation services.
- **Distributed middleware** – scalability, predictability, configurability and continuous commissioning,

- (D)GPS
- IIS active RFID,
- Symeo LPR,
- LETI UWB,
- CIT opportunistic localisation
- WiFi
- WSAN
- Cellular net.
Examples of control services:

- Continuous localisation of vehicles on the apron for safety and security
- Localisation of workers, sub-contractors, visitors for safety and security
- Location aware tasks allocation and scheduling
- Equipment and cars continuous commissioning
- Collision avoidance at the apron

(High accuracy - down to sub meter level)
Localisation systems used for indoor / outdoor

- (D)GPS
- IIS active RFID,
- Symeo LPR,
- LETI UWB,
- CIT opportunistic localisation
- Map Filtering
- Motion Models
Platforms & Devices

*Intelligent Embedded Sensing and Control Devices in Veneer (IQ Veneer)*

**Objective**
To develop, validate and demonstrate a process for embedding thin flexible electronics in veneers

**APPLICATIONS**
- Wall mounted security tag
- Information Containment
- Security alert surface
- Heated furniture/outdoor furniture
- Doors, floors in public areas
- Large area interfaces
- Recharging surfaces

*Touch Sensor Demonstrator*

*In Hand Guides*
- Audio guide with integrated eTicketing
- Wireless Location Aware Guide
eGo concept – EU CATRENE Project

- **What is it?**
  - A new way to establish a bidirectional secure, high-speed wireless channel between “objects”
  - Implemented in a secure portable device hosting all usual applications/credentials of a smart card

- **What is the form factor?**
  - Any form factor as a watch, a key ring, a jewel capable to host the eGo electronic

- **How it works?**
  - A unidirectional intra-body communication wakes up the eGo device and bootstrap a high speed wireless and bidirectional communication between eGo and an eGo compliant device

- **What do we get?**
  - A logical channel between eGo and an eGo compliant device which has been previously touched.

- **Market drivers**
  - Natural, no education needed, user friendly
**Nimbus’ role in eGo:**

**Demonstrators**

**Demo 1:** Identification & information access control

**Demo 2:** Healthcare

(entreainment system)

**Demo 3:** Internet of eGo devices

(access to multiple devices by touching one of them)

**Demo 4:** Car access

**Demo 5:** Electronic payment

**authorisation by touch**
Security Issues for Networked Embedded Systems

- Increasing use of networked embedded systems but with little attention to security
  - Complicated by standards uncertainty
  - Complicated by the large number of applications, e.g. energy, transportation and traffic, healthcare, etc.
  - Desire to connect everything to the Internet – “The Internet of Things”

- Security of networked embedded systems and information
  - Lately security attack on networked embedded control systems/SCADA/PLC
    - Security not an integral feature
  - Increasingly wireless systems
    - Offering sniffing based and jamming attacks
  - Information anonymity
Acknowledgements

- Colleagues
  - in NEMBES – HEA PRTLI4
  - in ITOBO – SFI funded SRC
  - In LocON – EU FP7
  - In eGO – EU CATRENE
www.nimbus.cit.ie

e-mail dirk.pesch@cit.ie

tel +353 21 433 5566