Open Networked CPSs

Networked, Cyber-Physical Systems that can be extended during operation by adding Apps on demand, e.g. for vehicles, medical devices, industrial automation

- Functional extension by Apps, as it is already common for mobile and other consumer devices
- Apps which can interact with safety-sensitive component by 3rd parties

**Pro**
- Enables products to keep pace with user expectations and latest features (eco-system)

**Cons**
- Apps imply new safety, privacy & security risks
Open Cyber-Physical Systems

Connectivity and new functionality (Apps) will be an integral part of the value proposition

• Consumers expect up-to-date, digital services

• “56% would switch to a different car brand if the one they were considering didn’t offer the technology features they want”, Autotrader.com survey, 2014
Security Challenges of Connected Cars

- Hackers Take Control of (moving) vehicles
  - Hacked Jeep Cherokee while driving
    - www.wsj.com/articles/hackers-show-they-can-take-control-of-moving-jeep-cherokee-1437522078
  - Tesla Model S
  - BMW Connected Drive hack, see heise.de
# Security and Safety for new Services

- Apps in vehicles to **add new functionality**
  - Apps require **open, flexible platforms** with access to car internals

- Need to ensure **safety and security** of the vehicle
  - Security means e.g. unauthorized actions
  - Safety issues may compromise proper operation of the vehicle

- **Security and safety** on existing, open platforms?
  - Abundant security issues for existing mobile platforms and Apps

<table>
<thead>
<tr>
<th>Vulnerabilities discovered in 2015</th>
<th># of issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Iphone Os</td>
<td>Apple</td>
</tr>
<tr>
<td>3 Flash Player</td>
<td>Adobe</td>
</tr>
<tr>
<td>19 Safari</td>
<td>Apple</td>
</tr>
<tr>
<td>20 Android</td>
<td>Google</td>
</tr>
<tr>
<td>21 Acrobat</td>
<td>Adobe</td>
</tr>
</tbody>
</table>

Source: http://www.cvedetails.com
Towards Trusted Automotive Apps

• Main requirements
  – **End-to-end trust chain** for deployment and apps management
    • Including access to **critical APIs**
  – **Highly trusted execution environment**
    • **Multiple, independent layers of security**

• **Current solutions separate** infotainment/apps HW from safety relevant control HW
  – Do not solve the problem of **access** to safety-critical resources (APIs)
  – Requires two physical platforms
TAPPS Approach: Multiple layers of security

1. **Trusted hardware** with security mechanisms
2. **Computing and network virtualization**
3. **Fine-grained access control** to resources to ensure safety and privacy (API checks, contracts).
4. **Verified, model-based Apps** to ensure correct and secure behavior.

blog.smartbear.com/design/what-medieval-castles-can-teach-you-about-web-security/
High-Level System Architecture

TAPPS Application Domains
Automotive
Healthcare
TAPPS Architecture for Open CPS Devices

End-to-end solution

Application Model

Apps Application Container

App Marketplace

toolchain

critical integration layer, Real-time Execution Environments

Rich EE

Trusted EE Virtualization, Inter-EE com

Critical EE Safety-integration layer, Real-time

Execution Environments

Normal World

ARM Trusted HW, ST WORM

Secure World

Secure CAN

Time Sensitive Networking

Trusted HW & Networks

TAPPS Device
Individual Protection Profiles via three Execution Environments

Towards Trusted Apps Platforms for Open CPS © fortiss GmbH
Validation

Trusted Apps Platform

Automotive domain
- check trip capability based on traffic conditions and battery status
- sport package changing driving behavior
- braking adjustment depending on environment conditions

Healthcare domain
- automatic drawers for safe drug management
- patient identification
- access to electronic health records
- monitoring of vital signs

C. Prehofer  www.tapps-project.eu
Summary

- TAPPS Project provides open platform with
  - Multiple layers of security
  - Execution environments with different protection level

- Challenges
  - Integrated security, safety, RT over all layers
    - From HW, NW, virtualization to SW
  - End-to-end security, boot, installation, operation,
  - Adaptation under real-time
  - ...

C. Prehofer

www.tapps-project.eu
Partners of TAPPS

Contact

www.tapps-project.eu
Security for Connected Devices – State of the Art

- Symantec report on security for Internet of things
  - "Around 19 percent of all tested mobile apps that are used to control IoT devices did not use Secure Socket Layer (SSL) connections to the cloud"
  - "The use of weak passwords is a security issue that has repeatedly been seen in IoT devices"
  - "Most of the IoT services did not provide signed or encrypted firmware updates"
  - "Conclusion: Any code that is run on a smart device, be it the firmware or application, should be verified through a chain of trust."

Source: http://www.symantec.com/iot/
Example State Machine
Active Suspension (simplified)

State     Actions     Output Events

Names qualified by service

INIT     INIT     INIT
1

STOPPED    STOPPED    STOPPED
1     2

ACC_RIGHT     ACC_RIGHT     ACC_RIGHT
2     4

ACC_LEFT     ACC_LEFT

DEC_LEFT     DEC_LEFT

DEC_RIGHT     DEC_RIGHT

V.VEL0=0

A.ACC>0

S.ANGLE=0

S.ANGLE>0

S.ANGLE<0

A.ACC<0

A.ACC>=0

S.ANGLE=0

S.ANGLE>0

S.ANGLE=0

S.ANGLE<0

S.ANGLE=0
Secure Apps by Design
Using a Model-based Toolchain

- 4DIAC: Established and standardized model-based toolchain from the industrial automation domain (IEC 61499)
- Code generation for TAPPS architecture
- Formal proof of Apps by model checking (NuSMV)
  - Test all possible executions
App Categories for Connected Cars

1. Pure **infotainment**, external services
   - Safety relevance is low

2. Apps which **access internal information**
   - E.g. address book, sensors, location, ....
   - Privacy issues, little safety issues

3. Integrated Apps which **modify internals**
   - E.g. customize vehicle dynamics (traction, ESP, ...) based on weather conditions
   - E.g. customize assistance systems
   - High demands on safety and security
   - May be **real-time critical**

Source: [http://kaddigart.deviantart.com/art/Apps-Box-1-Icon-334214248](http://kaddigart.deviantart.com/art/Apps-Box-1-Icon-334214248)
IEC 61499 Standard

- **Origin**
  - 1990s: holonic and agile manufacturing systems
  - Requirements: flexibility, adaptivity, and distribution

- **Goals**
  - Standardized architecture for function blocks in distributed industrial-process measurement and control systems
  - Basic support for dynamic reconfiguration

- Developed by IEC TC65/WG6, Started 1993

---

**Engineering Tool**

- Open Source, Eclipse Public License
- Components of solution
  - Engineering tool
  - Reusable component library

- Application domains:
  - Building automation, process industries, laboratory automation, smart grids, machine control, ...

- Core developers
  - fortiss GmbH
  - Profactor GmbH (AT)
  - Automation and Control Institute (ACIN)
  - Austrian Institute of Technology (AIT)

- Many users in industry and research/education