TAPPS - Trusted Apps for Open Cyber-Physical Systems

Christian Prehofer[1], George Kornaros[2], and Michele Paolino[3]

[1] fortiss, An-Institut Technische Universität München prehofer@fortiss.org
[2] TEI Crete, Informatics Engineering Dept. kornaros@ie.teicrete.gr
[3] Virtual Open Systems SAS, m.paolino@virtualopensystems.com

Abstract. Cyber-physical systems (CPS) are devices with sensors and actuators which link the physical with the virtual world. For CPS there is a strong trend towards open systems, which can be extended during operation by instantly adding functionalities on demand. The main goal of the TAPPS (Trusted Apps for open CPS) project is the development of a platform for CPS apps which can also access and modify safety critical device internals. As current, rich execution platforms for apps are limited in security, TAPPS will provide and validate an end-to-end solution for development and deployment of trusted apps. The project will develop a dedicated, real-time Trusted Execution Environment (TEE) for highly-trusted CPS apps. Additionally, TAPPS also includes an App Store and a model-based tool chain for trusted application development including verification tools. The multi-level trusted apps platform and tool chain are matured and validated in health and automotive application domains using industrial, realistic use cases paving the way for future exploitation in further demanding application domains.

1 Motivation and Approach

Cyber-physical systems (CPS) are devices with sensors and actuators which provide the link between the physical and the virtual world. An example is a connected vehicle able to read information from the road and combine it with cloud computing to provide new services to the driver. CPS are considered to be the next revolution in ICT with enormous economic potential enabling novel integrated services and products. In many areas of CPS devices, there is a strong trend towards open systems, which can be extended during operation by instantly adding functionalities on demand. In this area, the Trusted Apps for Open Cyber-Physical Systems (TAPPS) project focuses on the functional extension provided by apps, as it is already common for mobile and other consumer devices. However, there are considerable security issues for such devices. For example, a recent research work [2] reveals worrying results on this: in a dataset of 22500+ Android apps, 26% of their samples are identified as malicious. Considering now the sensitive interactions of CPS systems, including security, safety and privacy aspects, we see trust for such devices as a major societal challenge, which goes beyond the current role of computing in society [6].

The main goal of the TAPPS project is to extend and customize CPS devices with new 3rd party services and features in an efficient, secure and trusted apps platform. This extensibility is an important differentiator that enables new market extensions to keep pace with user expectations and latest technology. For instance, current apps for automotive vehicles provide infotainment functionality or control basic settings, both of which are not safety critical. As the next steps, apps targeting CPS devices can also use and adapt safety-sensitive functions, a concept which we call CPS apps. For instance, a sports upgrade package may change the driving behaviour of an automotive car, while another app may adapt the vehicle stability control according to road conditions. Similarly, in the health domain, we typically have vertical solutions for specific treatments. Here, we aim to open these towards multi-purpose devices, where apps may be installed for specific diagnosis or treatments. While such apps provide extra user value, there are considerable challenges for connected CPS devices regarding safety of the controlled system as well as safety and privacy of the user.

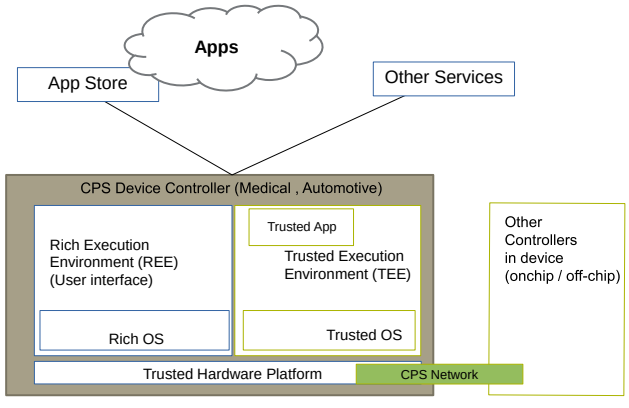

Fig. 1. Modern CPSs hosting both Rich and Trusted Execution Environments can provide services through an App Store without compromising platform security

As shown in Figure 1 in both automotive and medical domains, modern system architectures are open and distributed. While deploying corporate or 3rd party software through an App store provides simpler CPSs management and reduced system costs, adverse effects can be caused by direct interaction with safety critical settings, access to configuration APIs and misuse of system resources. As more sophisticated services and communication features are incorporated into CPSs any intentional or unintentional misuse that could compromise the platform should be prevented.

2 Research Challenges and Approach

To address the above, the TAPPS project goes beyond traditional solutions for safety, security and reliability in the CPS domain and offers a new approach to-

wards extensibility of CPS platforms. TAPPS is based on a dedicated, Trusted Execution Environment (TEE)[1] for distributed, safety-critical CPS applications. This is in addition to common rich execution environments (REE), which benefit from virtualization technologies and are oriented towards rich feature for applications. An overview of the TAPPS architecture and research challenges is shown in Figure 2. TAPPS offers multiple layers of security and an open end-to-end tool chain for developing and deploying trusted CPS apps.

TAPPS provides the following independent layers of security: First, computing and network virtualization based on novel, flexible hardware security mechanism, while maintaining stringent real time constraints in CPS devices and their internal networks. Secondly, fine-grained access control to resources of the smart cyber-physical device to ensure safety and privacy. Third, formally verified apps to ensure correct and secure behavior.

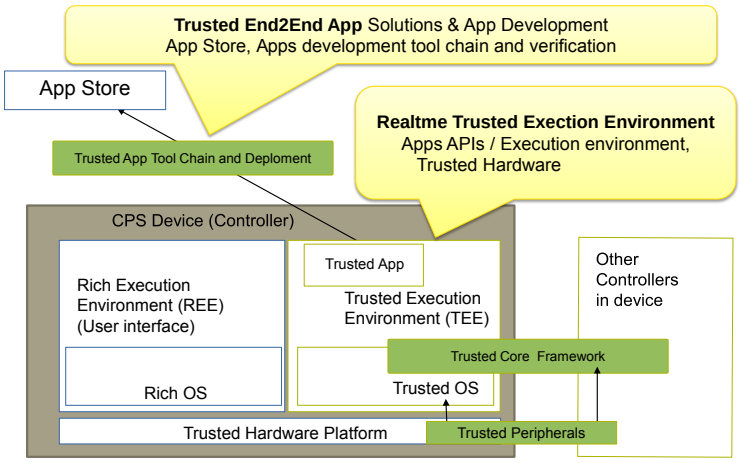

Fig. 2. TAPPS Overview and Research Challenges

The TAPPS TEE will be largely based on open source technologies, as pursued in the Automotive Grade Linux alliance (AGL) (www.automotivelinux.org), interacting with the open source community [3]. In parallel to the TEE, a Rich Execution Environment (REE) will be offered to execute the less critical parts of apps, e.g., the user interface of external interfaces. Only the small core of the critical functions is run in the new TEE, leveraging its native safety and security features.

The second main objective of the project is an end-to-end solution for development and deployment of trusted apps. This includes an application store for management of CPS apps and for deployment, supporting both the REE and the separate TEE. Furthermore, a model-based development tool chain for designing and implementing trusted apps including APIs and verification tools. Integration and active contribution to related open source model-based devel-

opment and verification tools is planned accordingly. The assumption is that we can check against unwanted behavior on the model level [5]. Using the deployment tool chain and App store, we ensure that only such checked code is running on the CPS device.

Finally, among the objectives is the creation of a realtime TEE for CPSs able to dynamically manage the various CPS partitions having mixed criticality requirements and supporting a trusted partition where different services can be securely executed. By using hardware enhancements for securing both on-chip ([4]) and off chip CPS networks, these can be mapped to the stacked layered network conceptual model. At the same time, in trusted Apps deterministic networks will be used to connect the distributed CPS with guaranteed behaviors such as a real-time communication possibility and guaranteed data exchange. Extensions to proven networking technologies (i.e., TTEthernet, CANbus) will ease the controlled exposure of CPS details such as sensor values towards non-trusted open networks such as the Internet/IoT.

In summary, TAPPS will provide and validate an end-to-end solution for development and deployment of trusted apps, including an app store and a model-based tool chain for trusted application development including verification tools. The trusted apps platform and tool chain are matured and evaluated in health and automotive application domains using industrial, realistic use cases paving the way for future exploitation in further demanding application domains.

References

1. GlobalPlatform. TEE system architecture v1.0. www.globalplatform.org, 2011.
2. A. Gorla, I. Tavecchia, F. Gross, and A. Zeller. Checking app behavior against app descriptions. In *ICSE'14: Proceedings of the 36th International Conference on Software Engineering*, 2014.
3. M. Paolino. ARM Trustzone and KVM coexistence with RTOS for automotive. http://events.linuxf oundation.org/sites/events/files/slides/als15_paolino.pdf, June 2015.
4. G. Kornaros, I. Christoforakis, O. Tomoutzoglou, D. Bakoyiannis, K. Vazakopoulou, M. Grammatikakis and A. Papagrigoriou. Hardware Support for Cost-Effective System-level Protection in Multi-Core SoCs. In *Euromicro Conference on Digital System Design (DSD)*, to appear, Aug 2015.
5. C. Prehofer. From the internet of things to trusted apps for things. In *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, pages 2037–2042, Aug 2013.
6. T. Tsiakis. The role of information security and cryptography in digital democracy:(human) rights and freedom. *Digital Democracy and the Impact of Technology on Governance and Politics: New Globalized Practices: New Globalized Practices*, page 160, 2013.