Project Information

ODSI

Project ID: C2014/2-12

Start Date: 1 November 2015

Closure date: 31 October 2018

Partners:

Beia Consult International, Romania

CityPassenger SA, France

Ingenieria del Poliuretano-Flexible, Spain

Innovalia Association, Spain

Internet of Trust, France

Nextel S.A., Spain

Orange SA, France

Prove & Run S.A.S., France

Resonate MP4 Romania, Romania

Software Quality Systems S.A., Spain

Université de Lille, France

Co-ordinator:

Patrick Picard

Orange SA

E-Mail: patrick.picard@orange.com

Project Website

www.celticplus.eu/project-odsi/

www.celticplus-odsi.org

On Demand Secure Isolation

The "On Demand Secure Isolation" (ODSI) project defines a new security model with isolation mechanisms and a new certification methodology to guarantee a high level of security for embedded products.

Moreover, new security mechanisms provide trusted support to propagate the isolation properties to remote management platforms for guaranteeing authorized accesses. (cf. Figure 1).

Main focus

Embedded systems have more and more complex architectures which increase the number of potential threats and attacks vectors.

In response to this complexity, ODSI project defines a new architecture relying on both hardware and software security solutions based on a light and proven isolation mechanism. This solution is available from the simplest device to the most complex equipment.

Thus, oriented towards simple hardware architecture, the most privilege code in the system is a Nano Kernel in charge of memory isolation. Then formal method demonstrates that this solution is mathematically proven.

Moreover, the security level of trusted systems is usually evaluated according to the Common Criteria certification processes. To reduce certification time and costs for complex systems ODSI introduces the composition method into the certification process to provide a kind of Lego mode certification methodology.

Different use cases demonstrate how the ODSI concepts could be implemented. Applications of ODSI concepts to Internet of Things (IoT) devices, Machine to Machine (M2M) equipment and also SCADA industrial systems are going to highlight the pertinence of increasing security thanks to ODSI project.

ODSI solution is composed of:

- Hardware: Set of electronic components which defines the device,
- Isolated area: Memory space completely independent from each other,
- Isolation Manager: Nano kernel Software entity able to provide proven isolated areas,
- Configuration manager: Software Entity able to manage isolated areas

ODSI remote Management platforms: Three platforms able to manage three

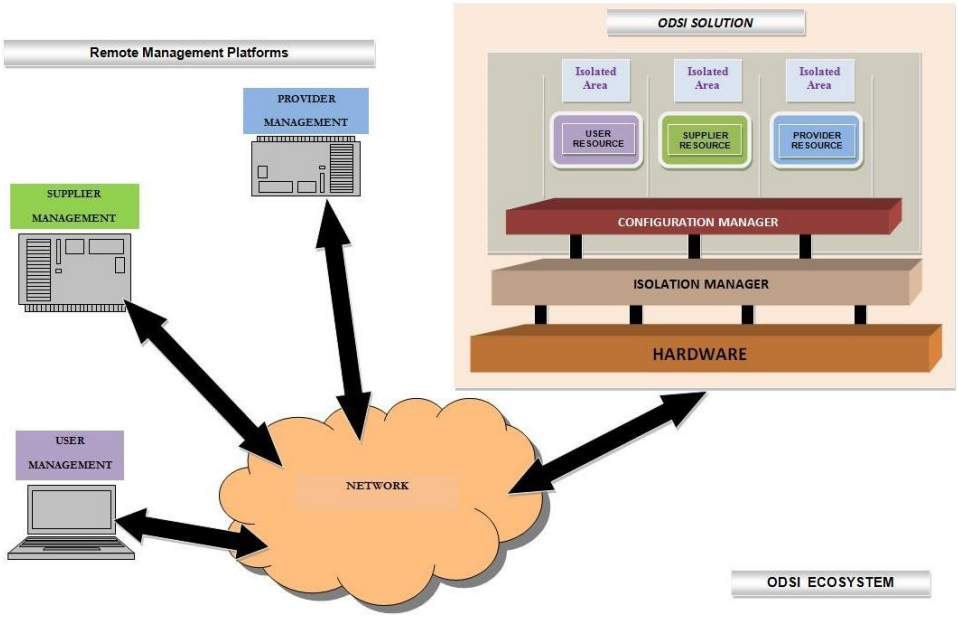

Figure 1: ODSI Ecosystem

resources of the ODSI solution

- One for the Supplier to manage supplier resources
- One for the Provider to manage provider resources
- One for the customer to manage customer resources

Approach

The massive deployment of Internet of Things devices, Machine to Machine (M2M) communications and the sharing of infrastructure pose real challenges in terms of security.

Today, the Industry offers only two alternatives for securing these new infrastructures: encryption of communications between equipment and flow monitoring. If encryption can prevent the looting of information, it will not prevent remote takeover of equipment from compromised equipment. Similarly, flow monitoring can never prevent any spread of compromise by an authorized flow, especially when it is encrypted.

So, the concepts developed by ODSI break with the current approaches. Thus, ODSI proposes to issue new architectures, for the simplest components, as well as for the most complex equipment, where security is provided by design based on a proven isolation mechanism.

This new hybrid security model combines both hardware and software security approaches. This choice is mainly based on an interoperability commitment providing the industry a low cost proven security model. Moreover, to propagate the isolation properties from a first isolated zone towards a second one, the project brings security mechanisms guaranteeing an authorised access to remote platforms.

Another dimension of the project is the optimization of Common Criteria certifications, which today are too heavy to meet the expectations of the industry. Reuse of all insurance levels already achieved on a set of systems to combine and compose in order to facilitate the assessment of a more complex system has not yet been demonstrated industrially. ODSI takes up the challenge and demonstrates it.

Main results

After specifying the ODSI concepts, practical examples show the usability of the new security models recommended by the project. These use cases have to convince that the results are fully compatible with most of the infrastructures.

The different developments apply the security isolation model through the three major domains that are embedded personal devices, IoT/M2M and networks. The isolation mechanism is first showing through a single device hosting both protected personal and professional environments.

The framework for Machine to Machine (M2M) and IoT interactions also sets up the isolation concept for a trusted remote access to the smart devices either in a factory for sensors, airport airside operations or agriculture domain for smart farming.

At last, two demos, one based on an industrial system able to remotely monitor and control processes and the other through the security of an advanced network system (routing, switching, etc.) will demonstrate the applicability of isolation properties and will highlight how the security level is improved by integrating ODSI specification.

Impact

ODSI delivers a proven abstract model of an Isolation Manager and its implementations on real platforms. This isolation reinforces sovereignty of infrastructures operators over their equipment, by providing a remote, safe and secure access to the system management of their platforms. Moreover, the issuance of minimal hypervisor on proven hardware targets to maintain research in the field of embedded security.

Through close cooperation with Certification Bodies, ODSI builds a new approach to Common Criteria methodology and a consistent attacks catalogue to certify efficiently IoT and M2M solutions. Then, with evaluation by composition and the reuse of certified bricks, a complete system can be evaluated at the highest assurance levels.

This enhances the deployment of any security device with the adequate assurance level in sensitive environments including critical infrastructures and reduces time-to-market in shortening and simplifying integration of certification processes.

To demonstrate the impact of ODSI, isolation security mechanisms are implemented in Industrial system to provide a trusted remote access to monitor and control the transportation and the storage of products. This will ensure a private and secure collection of data during all production processes.

About Celtic-Plus

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new „Smart Connected World“ paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the intergovernmental EUREKA network. Celtic-Plus is open to any type of company covering the Celtic-Plus research areas, large industry as well as small companies or universities and research organisations. Even companies outside the EUREKA countries may get some possibilities to join a Celtic-Plus project under certain conditions.

Celtic Office

c/o Eurescom, Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989 381
E-mail: office@celticplus.eu
www.celticplus.eu

EUREKA