Exploiting the security extensions of next generation CPUs for cloudifying critical applications

Luigi Romano – EPSILON srl
Roadmap

• Problem statement
  – Why real-time monitoring of water network infrastructures is important
  – Motivations for cloudifying a critical application
  – Issues of critical application cloudification

• The SERECA approach

• RiskBuster: real-time monitoring of water networks on secure clouds

• Achievements so far

• Plan for the future

• More info & contacts
Problem statement
Context

- Real-time monitoring of water network infrastructures is a key function for the society at large, since:
  - Water is key to virtually all human activities

Water is life, but ...
Water can cause terrible disasters

Water can take lives
Objective

- To provide a better and safer service to the community, by setting up an infrastructure for continuous monitoring of water networks.

- Typically, this would be implemented by means of traditional ICT technology, integrating SCADA (Supervisory Control And Data Acquisition) systems.
Issues

• The TCO (Total Cost of Ownership) of a traditional monitoring solution can be prohibitive, especially for organizations whose core business and technical skills are not in the ICT domain.

• Traditional solutions require an expensive ICT layer and data center infrastructure, which result in a major fraction of the cost.

• For such organizations, cloud computing has a dramatic potential in terms of cost reduction.

• This is exactly the case of SERECA partner EIPLI, a public administration that is in charge of water distribution in a large fraction of Southern Italy.

• However, real-time monitoring of water network infrastructures has challenging security and safety requirements, since the assets that must be protected are exposed to a variety of risks, ranging from accidental damage to criminal activities.
The SERECA approach
SERECA in a nutshell

• A security-enhanced cloud platform
• Exploits new Commercial Off The Shelf (COTS) CPU technology – notably: Intel SGX – for creating a protected environment that provides:
  – Secure processing
  – Secure communication
  – Secure storage
• Enhanced security is delivered to applications in a transparent way
• Compliant to OpenStack
RiskBuster: real-time monitoring of water networks on secure clouds
EPSILON RiskBuster pilot application

• Goals:
  – Infrastructure integrity monitoring
  – Key parameters monitoring (those with direct impact on the operation of the water network)
  – Water quality monitoring

• Achieved by:
  – Real-time data acquisition from a variety of sensors
  – Real-time data correlation and processing
  – Real-time alert generation and reporting
  – Long term storage of collected data
Conceptual Architecture
Achievements so far
1st prototype developed and tested

23/02/2016

1st DPSP project cluster workshop – Naples, February 23 2016
Plan for the future
To build a convincing Proof of Concept

- A full-fledged prototype will be deployed on a real dam infrastructure (most likely: the Monte Cotugno dam)
- The infrastructure will be instrumented with more sensors
- Sensor data will be published to SERECA vertx-based secure bus, using a permanent 4G connection
- Data streams will be processed in real-time by RiskBuster correlation engine
- Alerts will be generated in a timely fashion
- Collected data will be persisted using SERECA secure storage facilities
To make the transition to the field

• Making funds available to potential customers, i.e. to the Public Authorities that are in charge of water distribution

• The European Commission supports the transfer of research results to infrastructural improvements, and has provided mechanisms and guidelines for implementing synergies between H2020 and the European Structural and Investment Funds (ESIF)*

• Preconditions must be created: the local governments must include water network monitoring in their Smart Specialisation Strategy (S3)

• The SERECA Proof Of Concept (POC) will be used for persuading the local government of Puglia and Basilicata to do so

* http://ec.europa.eu/research/regions/index.cfm?pg=synergies
More info & Contacts
Project Overview

Cloud computing is nowadays a widespread technology that has been adopted in various fields thanks to the many well known benefits it offers. However there are still untouched areas, such as the case of Critical Infrastructures that monitor key parameters of water supply, electricity generation, or oil distribution.

What is really slowing down the integration between the cloud and the set of Industrial Control Systems (ICS) are security concerns.

Problem Statement: Cloud Security Threats

- A cloud stack is subjected to attacks at multiple levels (of the architectural layers)
- The most dangerous are those directed to the Hardware and the Hypervisor layers. These may allow the attacker to gain control of guests' Virtual Machines running on the host
- The shared technologies that permit the Multi-Tenancy cloud feature can be exploited by an attacker to open a security breach

Project Objective

http://www.serecaproject.eu/
SERECA Innovation Manager

Luigi Romano
EPSILON srl

email: prof.luigi.romano@gmail.com

mobile: +39 333 301 68 17
Acknowledgements & Disclaimer

SHERECA has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 645011

This presentation reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.