DKE WIPANO

UNIVERSITÄT SIEGEN

Naturwissenschaftlich-Technische Fakultät

Data Communications Systems

framatome

Attribute Based Access Control (ABAC for Smart Grid & IACS)

in Industrial Practice
ABAC / OPC UA / Virtualization

Ms. Asmaa Tellabi, *PhD Candidate, Framatome GmbH*

Dr. Karl Waedt, *Framatome GmbH*
Venesa Watson, *PhD Candidate*
Xinxin Lou, *PhD Candidate, Framatome GmbH*

Erlangen 2020-09-10

Personal information

- **Bachelor's Degree in Business Informatics** from Université international de Rabat in partnership with Université de Nantes, Morocco
- **Master's Degree in Information systems Security** from Université international de Rabat, Morocco
- **PhD Thesis at Framatome GmbH ICPGDA** since May. 2017
  - In cooperation with University of Siegen, Faculty of Communications,
  - Mentored by Prof. Christoph Karl Ruland
- **WINS Academy Ambassador since June 2020**
- **Member of R&D projects ABAC, SMARTEST and SMARTEST2**

Topics

1 . ABAC and OPC UA

2 . Mixed Criticality Systems

3 . ABAC with OPC UA and Virtualization

4 . Current Prototype Hardware and Software

5 . Summary and Outlook

1 . ABAC and OPC UA

Concepts

Address Space Model

OPC UA

- Industrial Machine to Machine (M2M) communication protocol for interoperability
  - for wireless and wired systems
  - M2M → integral part of the Internet of Things (IoT)

- Cross-platform Service Oriented Architecture (SOA) for Process Control
  - Enhanced Security, based on new standards
  - Based on different logical levels

- Provision of an Information Model

  Full Mesh Network based on Nodes

  Nodes → Processing of Data and Metadata

Source : OPC Foundation

Attribute Based Access Control Scope

Access Control against Insider Attacks

Source : Veronis

- Attributes are associated with **Subjects**, **Objects** and the **Environment**
  - ✓ ABAC allows to define more fine-grained access control rules

- ABAC can be used to design access control policies that make access decisions dependent on various parameters, including…

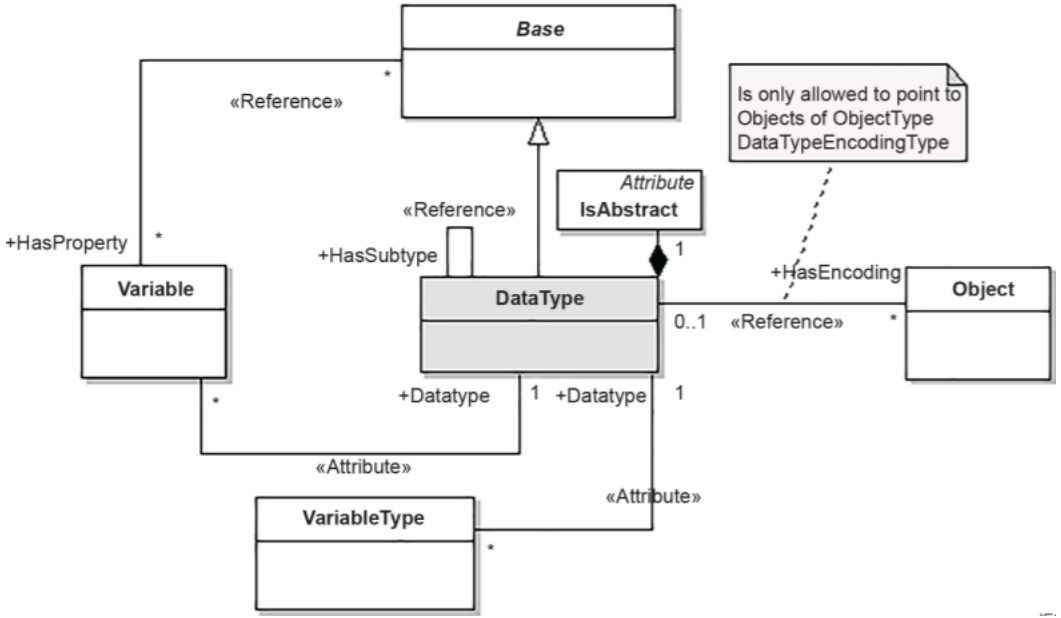
  - ✓ **Context**: Which is the context of the access request (Communication Association, System State, Security operational state, etc.)?

  - ✓ **Risk**: Which is the risk of the requested action?
    Which objects with which properties are accessed?
    The risk of an operation depends on request parameters and context.

ABAC Implementation
OPC UA Functionality / Address Space Model

- ABAC implementation using the
  - ✓ **Address Space Model** (IEC 62541-3)
  - ✓ **Information Model** (IEC 62541-5)

- If the functionality is not supported by the protocol
  - ✓ An **ABAC Firewall / Gateway** is needed
  - ✓ Acts as enforcement point for the ABAC policies



2 . Mixed Criticality Systems

System Architecture for Mixed Criticality

Attribute Based Access Control Context

Mixed Criticality Systems
Concepts

- They contain **two** or **more** software applications with different criticality
  - In case failures occur in higher-criticality applications unacceptable consequences may result, e.g., financial loss
  - The incorporation of MCS is becoming increasingly popular in the development of embedded systems
- When multiple functionalities are incorporated in the same system, it is expected that some of them will be more necessary for the system than others to ensure its activity

Source : InfoPreserve

ABAC Solution Development
Terminology

- Different levels of criticality are recognized by domain-specific standards:
  - DO-178B or ED-12B for avionics,
  - IEC 60880 for nuclear plants,
  - IEC 61400 for wind turbines
- To integrate MCS, an **isolation** mechanism between components on the single execution platform is required.
  - Mechanisms to realize such isolation include a **separation kernel** and **virtualization**

3 . ABAC with OPC UA and Virtualization

Virtualization

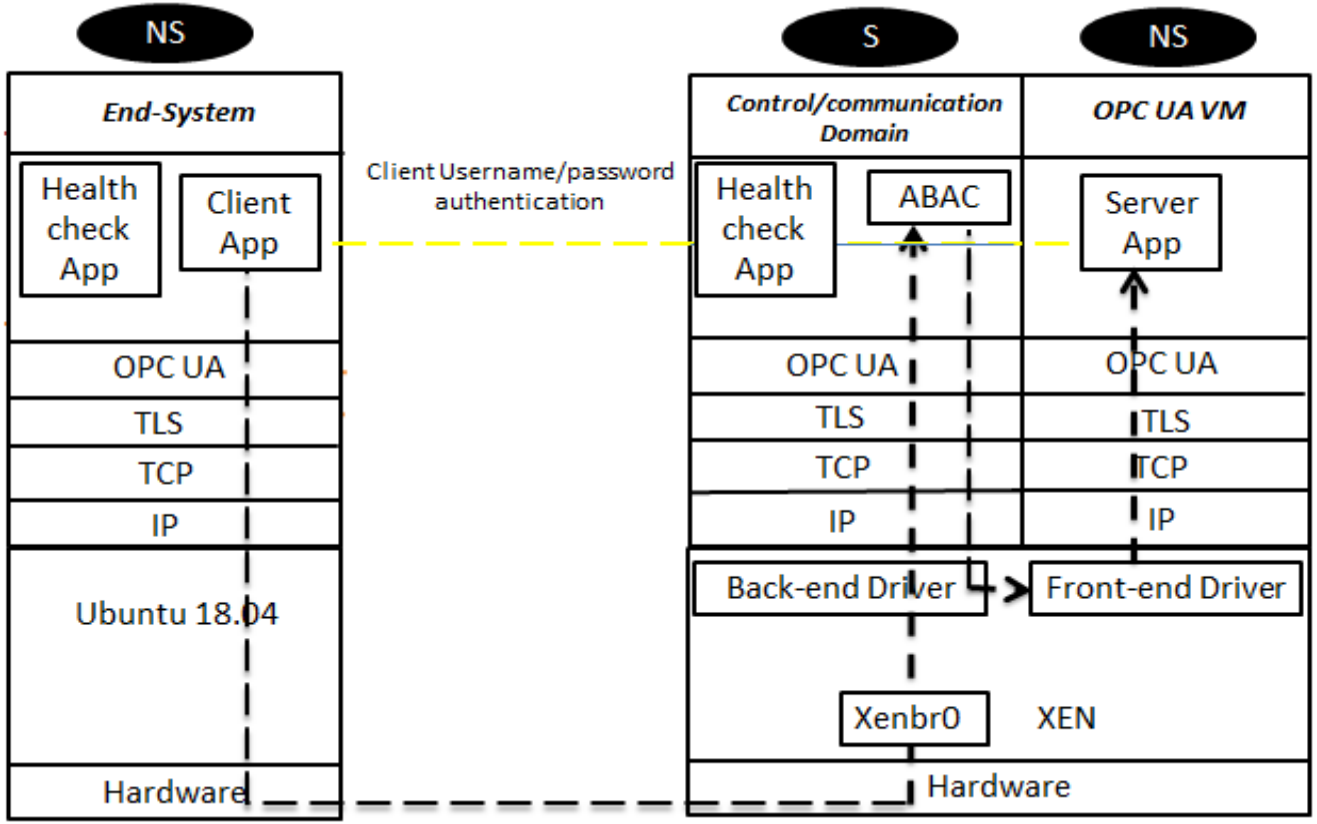
Definitions

- A set of simulated software and/or hardware above which another set of software operates, which is called a virtual machine (VM)
- A hypervisor is a layer composed of software, capable of running multiple different execution environments on a single computer
- It manages the hardware access and forms timing and spatial isolation between applications running on the same core
- it can be directly deployed on top of the hardware that is known as a bare metal hypervisor, or on top of an OS

4 . Current Prototype Hardware and Software

Architecture

Concepts



Source : LiliPutting

Architecture

Components

- Hypervisor
  - Xen which is an open source bare metal hypervisor
- Health Monitor check Application
  - To test the availability of the provided services
  - To check all the connected devices inside the network
- Client Application
  - Implements the OPC UA client using FreeOPCUA Library
- Server Application
  - Implements the OPC UA Server using FreeOPCUA Library
- **ABAC Software** integrated at OPC UA Server side

Architecture

Requirements

Source : Xen

- The idea behind the design of this system is to create a single point entrance from the outside world (Internet) to the inside world (Domains)
  - Domain 0 is responsible of controlling the communication flow between the Non-secure Domain and the secure Domain
  - The Non-secure Domain should not be connected to internet
  - All requests coming from the client should not be transmitted directly to the Server, they should be treated the Domain 0 and then transmitted to the server

4 . Summary and Outlook

Conclusions

- Virtualization permits the execution of several OSs and applications
  - at the same time (concurrently)
  - but isolated from each other
  - on a single physical host hardware

- Approaches for alternative types of virtualization differ BUT They do hold in common the approach of breaking limitations of the physical hardware
  - by creating secure partitions inside the hardware
  - similar to multiple virtual environments

- The **ABAC solution developed in the R&D project** can be integrated at the server side into the virtual environment
  - ABAC prototype for OPC UA server side being completed soon
  - Client side being prepared for industry grade applications

framatome

Thank you