Components of Attribute based Access Control

Firewall with attribute based access control

Microcomputer with Linux, particularly assigned for legacy systems, which are not able to be extended by new access control mechanisms

Attribute based access control can also be integrated in Intelligent Electronic Devices (IEDs, control units)

Additionally, the following are offered:

Attribute Certificate Management System

- For generation of attribute certificates for access permitted users and processes
- For generation of attribute certificates for system components and objects to be accessed

Policy Management System

- For generation of rules, which specify the access requirements
- Configuration of system states to be considered by the rules, resp. access requirements

LDAP-Server

- For provision of X.509 certificates issued by a Certification Authority (CA)
- For provision of all attribute certificates
- For provision of access rules (Access Control Policies)
  by application of Push- or Pull-methods.

Chair for Data Communications Systems

Since 1992 the Chair for Data Communications Systems of the University of Siegen researches and works on the integration of security and cryptographic mechanisms in digital communications systems, with focus on real time and industrial scenarios. Until now, the following has been performed in this area:

- 38 dissertations (Dr. degrees)
- 13 EU-Projects
- 5 DFG-Projects (German national research organization)
- Many projects funded by governmental institutions and industrial partners.

The Chair is a member of:

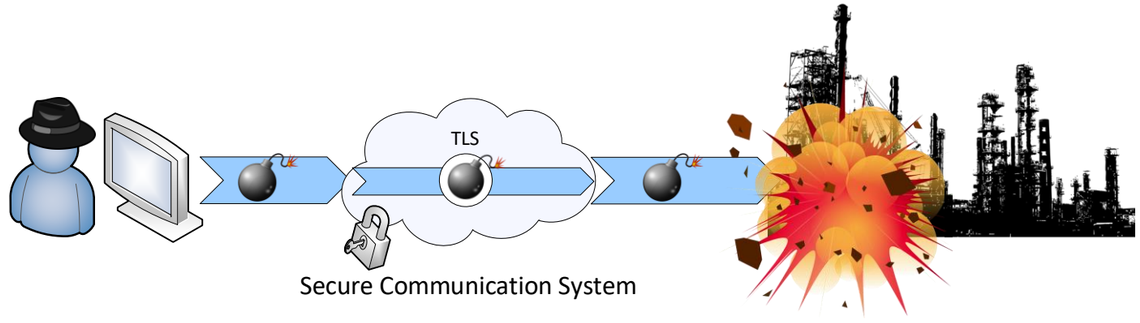
- ISO SC 27 Security Techniques and DIN AA 27
- IEC TC 57 Power systems management and associated information exchange and DKE AK 952

Contact

University of Siegen
Prof. Dr. Christoph Ruland, christoph.ruland@uni-siegen.de, Tel. +49 271 740 2522
Jochen Sassmannshausen, jochen.sassmannshausen@uni-siegen.de Tel. +49 271 740 3325

IMPROVED PROTECTION AGAINST INTERNAL ATTACKERS IN DISTRIBUTED INDUSTRIAL SYSTEMS BY

ATTRIBUTE BASED ACCESS CONTROL



Internal Attackers/insiders have permitted access to critical systems and can cause damages of infrastructures, humans and environments despite of the usage of secure communications

Applications

- Energy Generation and Distribution (Smart Grid)
- Industrial Internet of Things (IIoT)
- Industry 4.0/Smart Manufacturing
- eHealth
- Transport and Logistics

Situation

By introduction of new concepts of distributed communications in industrial supervisory and control systems the number of users and processes with access permissions is dramatically increased, and therefore also the number of potential internal attackers. Examples are Smart Grids with the integration of decentral energy generation, Industrial Internet of Things (IIoT) und Smart Manufacturing/Industry 4.0, which may include the complete supply chain and logistics.

Risks by Insiders and Internal Attackers

Internal attackers possess certain access permissions inside of a system. By exceeding, unauthorized usage or misusage of these access rights irreparable damages and catastrophes for humans, environment and infrastructures can be caused. When external attackers succeed to intrude into an internal network, they appear as internal attackers as well.

Security Solution

Attribute based access control is performed subject- and **object** oriented. The permission of access is dependent on the risk potential of the object or the parameters value included in a control command. Access rules are specified for each object and its allowed parameter values. Additionally, access control is dependent on the actual system state.

UNIVERSITÄT SIEGEN
Chair for Data Communications Systems
Univ.-Prof. Dr. Christoph Ruland
University of Siegen, Hoelderlinstrasse 3, 57076 Siegen
https://www.eti.uni-siegen.de/dcs/

System Architecture and Components

Device Data Model
iedModel
TTMP1
TmpSv
TTMP2
...

Attribute Certificate
Holder: iedModel/TTMP1

Attributes:
Type: Temperature Sensor
Criticality: Low

Users
User 1
Administrator
...

Attribute Certificate
Holder: User 1

Attributes:
Role: Operator
AoR: Substation xyz

Certificate Authority
Issues Public Key Certificates to components, processes and users

Attribute Certificate Management

Issues Attribute Certificates for Users and Data Objects

Signed Attribute Certificates and CRL Updates

Policy Management

Select Target IED

Configuration for target IED

Select Profile

Profile 1
Profile 2
...
Profile n

Profile content

System Config.

SHA-256
SHA-256
SHA-256

XACML Policies
System State Specification
Context Sensitive Policies

Each element is digitally signed with the Policy Management private key

Signed Policies and System Configuration

LDAP Node

CRL
User Attributes
Access Control Policies
Object Attributes

LDAP Server

The Data Model and Access Control Policies of each Device are represented by individual subtrees on the server

Synchronization using LDAP Persistent Search (i.e. LDAP SYNC) and pull on demand (e.g. for user Attribute Certificates)

Processes and Users obtain their Attribute Certificates from the LDAP Server (Pull)

End-to-End Security
(Push Credentials)

e.g. IEC 61850

e.g. IEC 61850

Client access
(e.g. via HMI)

Attribute-based Access Control Firewall

Legacy Devices

Equipment