Komponenten der Attributbasierten Zugriffskontrolle

Firewall mit attributbasierter Zugriffskontrolle

Mikrocomputersystem mit Linux, besonders geeignet für Legacy-Komponenten, in denen die Zugriffskontrolle nicht integriert werden kann.

Optional kann diese auch in Intelligent Electronic Devices (IEDs, Steuergeräte) integriert werden.

Dazu werden angeboten:

Attribute Certificate Managementsystem

- Zur Erstellung der Attributzertifikate für zugriffsberechtigte Teilnehmer und Prozesse
- Zur Erstellung der Attributzertifikate für die Systemkomponenten und Objekte, auf die zugegriffen werden soll

Policy Managementsystem

- Zur Erstellung aller Regeln, nach denen der Zugriff erfolgen soll
- Konfiguration der Systemzustände, die in den Regeln berücksichtigt werden sollen

LDAP-Server

- Zur Bereitstellung der X.509 - Zertifikate, die von einer Zertifizierungsinstanz ausgestellt werden
- Zur Bereitstellung aller Attributzertifikate
- Zur Bereitstellung der Zugriffsregeln (Access Control Policy)

über Push- oder Pull-Mechanismen.

Lehrstuhl für Digitale Kommunikationssysteme

Der Lehrstuhl für Digitale Kommunikationssysteme der Universität Siegen arbeitet seit 1992 auf dem Gebiet der Einbindung von Sicherheit und Kryptographie in digitale, insbesondere realzeit- und industrielle Kommunikationssysteme. Auf diesem Gebiet wurden bisher

- 38 Promotionen
- 13 EU-Projekte
- 5 DFG-Projekte
- Drittmittelprojekte mit Behörden, Ministerien und Industriepartnern durchgeführt.

Der Lehrstuhl ist Mitglied in Normungsausschüssen der

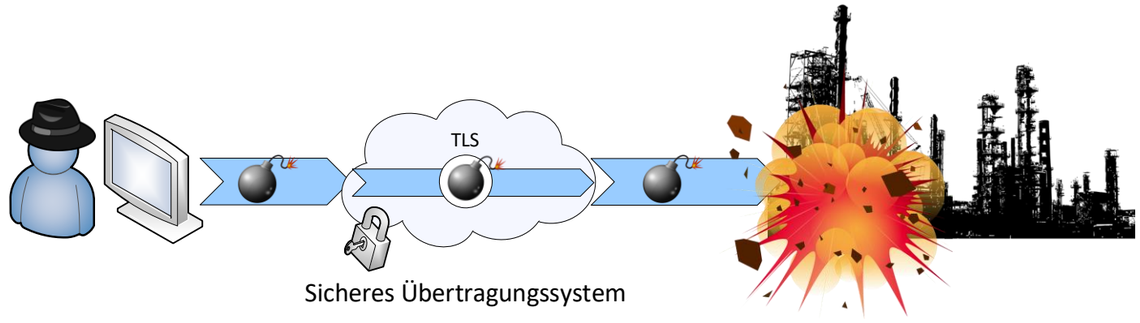
- DIN/ISO SC 27 Security Techniques
- IEC TC 57 / DKE AK 952 Netzleittechnik

Ansprechpartner

Universität Siegen
Prof. Dr. Christoph Ruland, christoph.ruland@uni-siegen.de, Tel. 0271 740 2522
Jochen Saßmannshausen, jochen.sassmannshausen@uni-siegen.de Tel. 0271 740 3325

VERBESSERTER SCHUTZ GEGEN INNENTÄTER IN VERNETZTEN INDUSTRIELLEN SYSTEMEN DURCH

ATTRIBUT-BASIERTE ZUGRIFFSKONTROLLE



Innentäter haben befugten Zugang zu sensiblen Systemen und können trotz gesicherter Übertragung Schäden an Infrastrukturen, Mensch und Umwelt verursachen

Anwendungsbereiche

- Energieverteilung und –steuerung (Smart Grid)
- Industrial Internet of Things (IIoT)
- Industrie 4.0/Smart Manufacturing
- eHealth
- Transport und Logistik

Situation

Durch neue Konzepte der Vernetzung in industriellen Steuerungssystemen ist die Anzahl der befugten Teilnehmer und damit der potentiellen Innentäter unübersehbar geworden. Beispiele sind Smart Grids im Rahmen der dezentralen Energieerzeugung, Industrielles IoT und Smart Manufacturing/Industrie 4.0, bei denen die gesamte Supply Chain und Logistik integriert werden können.

Gefahren durch Insider und Innentäter

Innentäter verfügen über gewisse Zugriffsrechte innerhalb eines Gesamtsystems. Durch Überschreitung, unbefugte Anwendung und Missbrauch dieser Rechte können große irreparable Schäden und Katastrophen für Mensch, Umwelt und Infrastrukturen verursacht werden. Wenn externe Personen in ein internes Netz eindringen, zählen sie ebenfalls als Innentäter.

Sicherheitslösung

Die Attributbasierte Zugriffskontrolle arbeitet subjekt- und **objektorientiert**. Der Zugriff wird von dem Risikopotential des Zielobjektes oder der Parameterwerte in einem Steuerungsbefehl abhängig gemacht. Für jedes Objekt und seine möglichen Parameterwerte werden Zugriffsregeln spezifiziert. Zusätzlich erfolgt die Zugriffskontrolle abhängig von dem aktuellen Systemzustand.

UNIVERSITÄT SIEGEN
Lehrstuhl für Digitale Kommunikationssysteme
Univ.-Prof. Dr. Christoph Ruland
Universität Siegen, Hölderlinstraße 3, 57076 Siegen
https://www.eti.uni-siegen.de/dcs/

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

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
XACML Policies
SHA-256
System State Specification
SHA-256
Context Sensitive Policies
Each element is digitally signed with the Policy Management private key

Signed Policies and System Configuration

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

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