Das ABAC-Projekt
- Hintergründe und Ziele -

Christoph Ruland

ABAC Workshop des DKE
„Feingranulare Zugriffskontrolle“

DKE - Virtueller Seminarraum, 10. September 2020

Kommunikationssicherheit – notwendig, aber nicht hinreichend

Bisher:

- Sicherheitsmechanismen und -Protokolle auf den Schichten des Transportsystems, z.B. Schicht 2 (MACSEC), Schicht 3 (IPSEC), Schicht 4 (TLS)
- Sicherheitsdienste: Authentizität der Teilnehmer, Authentizität der Daten, Datenintegrität, Vertraulichkeit

Aber:

- Sicherheitsdienste gelten für **alle** Dateninhalte, auch für unerwünschte und böswillige
- Schützen nur vor externen Angriffen während der Übertragung
- Schützen nicht vor internen Angriffen
- Externe Angreifer haben nach Überwindung der Firewall Rechte wie interne Angreifer

Neuer Ansatz:

- Das Risiko einer Transaktion hängt von der Bedeutung des Dateninhaltes ab
- Nur die Anwendung kennt die Bedeutung und Wirkung
- Sicherheit muss die Bedeutung des Dateninhaltes und das Objekt berücksichtigen, auf das sich die Dateninhalte beziehen

Kommunikationssicherheit ist notwendig, erst mit Anwendungssicherheit hinreichend

Übliche Sicherheitssysteme nicht ausreichend

- User-ID und Passwort – evtl. sogar unverschlüsselt
- Firewall
- Authentikation bei Verbindungsaufbau: **Man-in-the-Middle**-Attacken auf Datenaustausch
- TLS: Unter Umständen nicht End-to-End, bietet auch nur Schutz des Transportes
- TLS: Zertifikatsinhaber muss nicht der Identität des Anwenders entsprechen
- Keine Nachweisbarkeit

Neue Ansätze für Sicherheit auf der Anwendungsebene

- IEC 62351-4 (End-to-End-Security für MMS), IEC 62351-6 (Security für IEC 61850)
- OPC UA (IEC 62541): Teil 4 (Services) und Teil 6 (Mapping) beinhalten End-to-End Security-Mechanismen

Trend

Sicherheitsprotokolle auf der Anwenderschicht mit eigenen Authentifikationsprotokollen zwischen den tatsächlichen Anwendern, z.B. Subjekt und Objekt, unabhängig davon, ob bereits Kommunikationssicherheit gegeben ist, z.B. TLS

Ziel: Einführung objektorientierter Sicherheit

- Bisher überwiegend subjektorientierte Sicherheit: Befugnisse werden an die Person oder Rolle gebunden, die aktiv werden soll
- Das Risiko der Aktivität hängt aber davon ab, was das Subjekt ausführen will, d.h. auf welches Objekt es zugreifen will und wie es dieses modifizieren will
- Die Sicherheitsanforderungen müssen abhängig vom Objekt und den möglichen Auswirkungen der Operationen festgelegt werden
- Sicherheitsanalyse erforderlich
- Es ist eine feine Granularität erforderlich, da die Risiken von Details abhängig sind, z.B. Parameterwerten

Lösung: Objektorientierte attributbasierte Zugriffskontrolle

- Nicht ganz neu (NIST SP 800-162 (2014,letzte Version 2019): Guide to Attribute Based Access Control (ABAC) Definition and Considerations)
- Die Subjekte erhalten Attribute, die z.B. ihrer Rolle entsprechen (RBAC)
- Die Sicherheitsattribute werden z.B. in Form von Attributzertifikaten ausgestellt (X.509)

Neu bei ABAC

- Sicherheitsattribute für die Objekte
- Objekte sind in einem Datenmodell organisiert, das ggf. auch semantische Informationen enthält
- Feingranulare Zuteilung der Zugriffsrechte entsprechend der (Teil-) Struktur des Datenmodells
- Sicherheitsattribute werden unter Berücksichtigung von Risikobetrachtungen vergeben

Access Control Policy

- Durch befugte Administratoren festgelegt
- Befugnisse der Subjekte müssen zu Einstufungen der Objekte passen
- Ähnlich zu Bel la Padula und militärischen Systemen, jetzt aber **viel feingranularer, nicht nur wenige, pauschale Klassifikationen**
- **Zusätzlich:** Anwendung der Zugangsregeln abhängig vom Systemzustand und mit Gedächtnis

Das WIPANO-Projekt – Attribute-based Access Control für IEC 61850

Warum IEC 61850?

- IEC 61850 gilt als das zukunftsträchtigste Protokoll für Smart Grids
- IEC 61850 verwendet (hierarchische) Datenmodelle, die sich besonders gut für objektorientierte Sicherheit eignen
- IEC 61850 liefert mit dem Datenmodell semantische Informationen über die Objekte
- IEC 61850 stellt Service-Schnittstellen zur Verfügung, über die z.B. das Datenmodell abgerufen werden kann

Warum Smart Grid?

- Besonderer Handlungsbedarf, da Smart Grids zu den sicherheitskritischen Infrastrukturen gehören und ständig im Ziel von Angriffen stehen
- Die Zusammenlegung von isolierten Energieverteilungssystemen zu Smart Grids stellt zahlreiche neue Sicherheitsanforderungen

WIPANO

Programm des Bundesministerium für Wirtschaft und Energie zur Förderung des Wissenstransfers in Patente und Normung

Ziel des WIPANO-Projektes: Attribute-based Access Control für IEC 61850

- Einbringung der Technologie der attributbasierten Zugriffskontrolle in die nationale und internationale Standardisierung
- Aktivitäten zur Standardisierung einer Erweiterung von IEC 61850, bzw. IEC 62351
- Mitarbeit in DKE 952 (Netzleittechnik), 0.10, (Kommunikation und Modellierung) sowie IECTC 57 WG 10 und 952.0.15 (Informationssicherheit in der Netz- und Stationsleittechnik), sowie IEC TC 57 WG 15

Projektpartner

- Universität Siegen, Lehrstuhl für Digitale Kommunikationssysteme
- Framatome (Industriepartner)
- DKE (Transfer in Standardisierungsgremien und Verbände)

Projektlaufzeit: 1.10.2018 – 30.9.2020

Quo Vadis, ABAC?

aus Sicht der Universität Siegen

1. Verlängerung des WIPANO-Projektes um 6 Monate, da einige Sitzungen ausgefallen sind und die Standardisierung weiter unterstützt werden soll

2. Integration in OPC UA (bereits auf eWorld 2020 demonstriert)

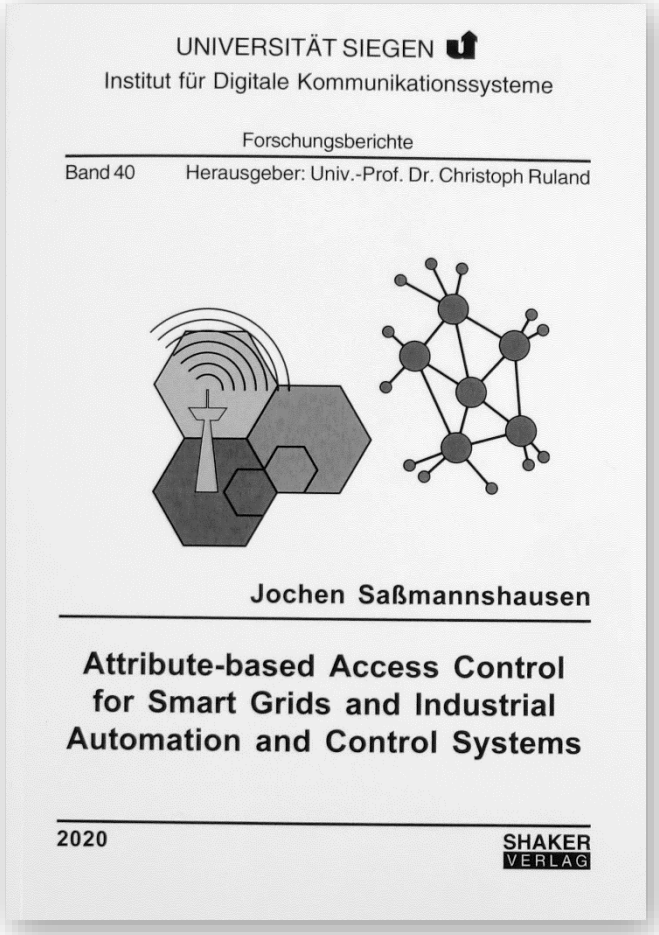
3. Integration in IACS (Industrial Automation and Control Systems) und Industrie 4.0

4. Neues strategisches Projekt des BMWi im Bereich „Entwicklung Digitaler Technologien“

   „Sichere und robuste kalibrierte Messsysteme für die digitale Transformation“,

   in dem ABAC ebenfalls zum Einsatz kommt

Dokumentation der Technologie und ihrer Umsetzung



Vielen Dank

für Ihr Interesse an ABAC

und den weiteren Vorträgen unseres Workshops !

Fragen gerne per Audio oder Chat