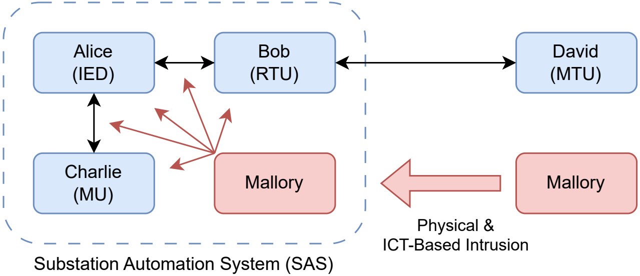
Karlsruhe Institute of Technology

Certificateless Attribute-Based Server-Aided Cryptosystem for Substation Automation Systems (CASC-SAS)

Master’s Thesis Presentation

Moritz Gstuer | 12. February 2025

Motivation



Cyberattacks

- **Availability-Focused:** Denial-of-Service
  → Malware, Flooding, & Time-Delay
- **Integrity-Focused:** False Data Injection
  → Message Forgery, Modification, & Replay
- **Authenticity-Focused:** Masquerading
  → Adaptive Chosen-Message, & Collusion

IED. . . Intelligent Electronic Device | RTU. . . Remote Terminal Unit | MTU. . . Master Terminal Unit | MU. . . Merging Unit
ICT. . . Information and Communications Technology

Substation Communication

Requirements

- Integrity
- Authenticity
- Non-Repudiation

→ **Authentication**

- Prevention of Unauthorized Access
- Least Privilege Principle
- Separation of Duties

→ **Authorization & Access Control**

Constraints: IEC 61850 Message Types & Performance Classes (2014; 2022)

Client-Server (Unicast) & Publisher-Subscriber (Broadcast/Multicast)

→ Resource & Time Constraints!

Examples: GOOSE (Type 1A, 3 ms), SV (Type 4, 3 ms), MMS (Type 2/3/5, 100-10000 ms)

GOOSE. . . Generic Object Oriented Substation Event | SV. . . Sampled Values | MMS. . . Manufacturing Message Specification

Research Questions

RQ 1: Authorization & Access Control in Substation Automation System

How can **expressive** and **flexible** yet computationally expensive **access control** be employed in a SAS?

RQ 2: Public-Key Cryptography in Substation Automation System

How can a **secure** and **lightweight public-key approach** be designed, implemented, & employed in a SAS?

RQ 3: Security Architecture for Time-Critical Communication

How can **authentication**, **authorization**, and **access control** be integrated into a malleable, scalable, and lightweight **cryptosystem for time-critical SAS communication**?

Attribute-Based Access Control (ABAC)

Definition (Task Force Interagency Working Group 2020)

Access control model enabling access decisions based on attributes associated with **subjects**, **objects**, **actions**, and the **environment** of a system.

Discussion (Hu et al. 2014)

- Multifactor Policy Expression → Fine-Grained & Flexible Access Control (cf. RBAC/IBAC)
- Dynamic Policy Evaluation → Dynamic Authorization & Real-Time Attributes

Public-Key Cryptography in SAS

Key Distribution & Identity Verification

Unsecure Network & Untrusted Network Participants
→ Asymmetric: Lightweight & Secure Key Distribution

Computational Complexity (Elbez et al. 2019; Ishchenko and Nuqui 2018)

Example: 1024-Bit RSA Digital Signature vs. 128-Bit HMAC/GMAC
→ 10 ms vs. 50 µs on RPi2 (1 GHz quad-core)
→ 0.3 ms vs. 4 µs on Xeon X3440 (2.53 GHz quad-core)

Norms & Standards

IEC 62351: Part 6 & Part 8 (2020a; 2020b)

Standard for Cybersecurity: Energy-Related Systems & Communication Networks
→ **Authenticity & Integrity:** Mandatory Symmetric Authentication
→ **Confidentiality:** Optional (Non-Recommended) Symmetric Encryption
→ **Access Control:** Role-Based Access Control (RBAC) (Access-Token-Driven, 7 Mandatory Roles)

Related Work

Secure Communication in Substations

- Bump-in-the-Wire Security Filter for **GOOSE/SV MAC Tagging** & Verification (Ishchenko and Nuqui 2018)
- **Domain-Based Collaborative** Cyberattack Mitigation Approach (Hong et al. 2019)
- Fixed-Latency Hardware Architecture for **GOOSE/SV Encryption** & Authentication (Rodriguez et al. 2021)

Access Control in Substations

- XACML-Based **RBAC** Approach for IEC 61850 & IEC 62351 compliant SAS (Lee et al. 2015)
- Distributed **RBAC** for Subscription-Based Remote Network Services (Ma and Woodhead 2006)
- Rule-Based **RBAC** Policy Enforcement Architecture (Alcaraz et al. 2016)
- Firewall for **ABAC** in Smart Grids (Ruland and Sassmannshausen 2018)
- **ABAC** for Real-Time Availability in Highly Dynamic Systems (Burmester et al. 2013)

Research Gap & Contributions

Limitations of Related Work

Missing consolidation of secure communication & access control in substations
→ **Consolidation of Competencies:** Increase security & performance, & facilitate deployment

Contributions

- Requirements & constraints of the **field of application**
- **Authorization** & **access control** approach based on ABAC → **RQ 1**
- Algorithm-agnostic **authentication** framework & attribute-based signature scheme → **RQ 2**
- **Security architecture** integrating authentication, authorization, & access control → **RQ 3**
- Security, performance, & compatibility **evaluation** of the approach

Approach: Overview

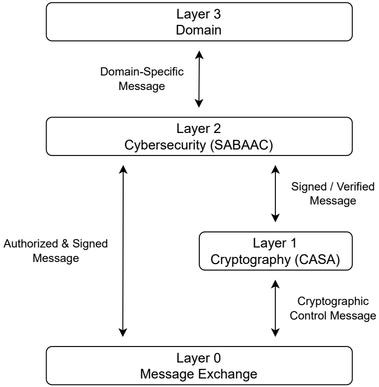
Approach

Certificateless **A**ttribute-Based **S**erver-Aided **C**ryptosystem for **S**ubstation **A**utomation **S**ystems (CASC-SAS)

Objective: Fine-grained & flexible access control relying on dynamic authorization & authentication

Central Concepts:

- Authentication → CASA
- Authorization & Access Control → SABAAC



CASA. . . Certificateless Attribute-Based Server-Aided Authentication
SABAAC. . . Server-Aided Attribute-Based Authorization & Access Control

CASA: Authentication

Certificateless **A**ttribute-Based **S**erver-Aided **A**uthentication (CASA)

Lightweight & scalable algorithm-agnostic data frame authentication approach

Additionally: $S_{CASA} \rightarrow$ Certificateless attribute-based server-aided signature scheme

Protocol: Algorithm-Agnostic PKC Exchange

Tasks: Registration, revocation, query, & computation

Central Component: CASA Administration and Processing Platform (CAPP)

PKC. . . Public Key Cryptography

SABAAC: Authorization & Access Control

Server-Aided **A**ttribute-**B**ased **A**uthorization & **A**ccess **C**ontrol (SABAAC)

Delegation of access policy evaluation to semi-trusted server (PDP)
→ Enforcement of access control decisions via bump-in-the-wire device (PEP)

Protocol: Delegated Attribute-Based Authorization

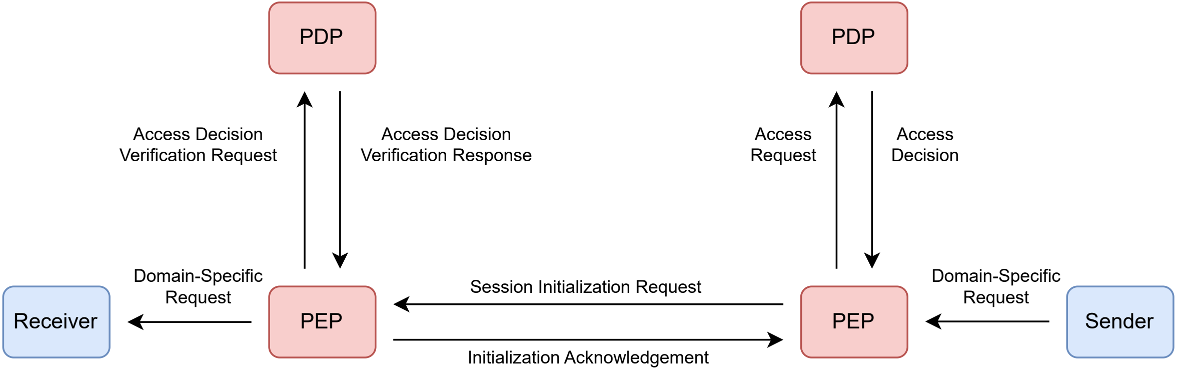
Task: Creation, modification, storage, and distribution of access control policies
Central Components: PAP & PDP

Protocol: Delegated Attribute-Based Access Control

Task: Request, exchange, & enforcement of access control decisions
Central Components: PDP & PEP

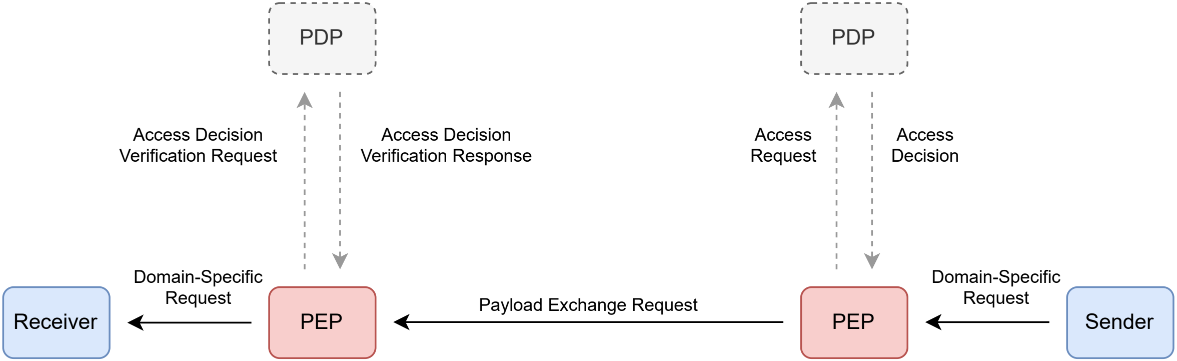
PAP. . . Policy Administration Point | PDP. . . Policy Decision Point | PEP. . . Policy Enforcement Point

Delegated Access Control: Session Initialization


PDP
PDP
Access Decision Verification Request
Access Decision Verification Response
Access Request
Access Decision
Domain-Specific Request
Receiver
PEP
Session Initialization Request
Initialization Acknowledgement
PEP
Domain-Specific Request
Sender

PDP. . . Policy Decision Point
PEP. . . Policy Enforcement Point

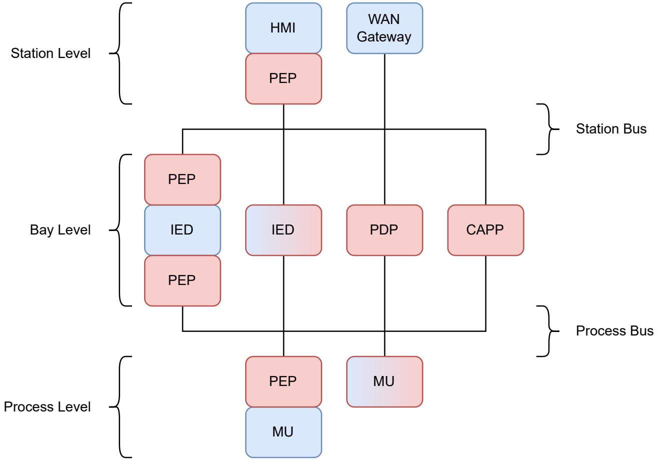
Delegated Access Control: Payload Exchange



PDP... Policy Decision Point

PEP... Policy Enforcement Point

CASC-SAS: Component-Oriented Architecture



CAPP	CASA Administration & Processing Platform
PDP	Policy Decision Point
PEP	Policy Enforcement Point
HMI	Human-Machine Interface
IED	Intelligent Electronic Device
MU	Merging Unit
WAN	Wide Area Network

Evaluation: Overview

Goal of Approach

Protect substations against domain-typical adversaries & attacks

Communication: Time-Constrained & Traffic-Intensive

Deployment: Construction & Retrofitting

Evaluation

Theoretically & experimentally performed evaluation

- Security Analysis
- Performance Analysis
- Compatibility Analysis

Security Analysis

Central Question

To what extent does CASC-SAS provide security against typical SAS adversaries and attacks?
Metrics: Satisfied requirements, assumed adversary, mitigated attacks, & change of substation attack surface

Theorems

Demonstration of the reduced likelihood and impact of six attacks:

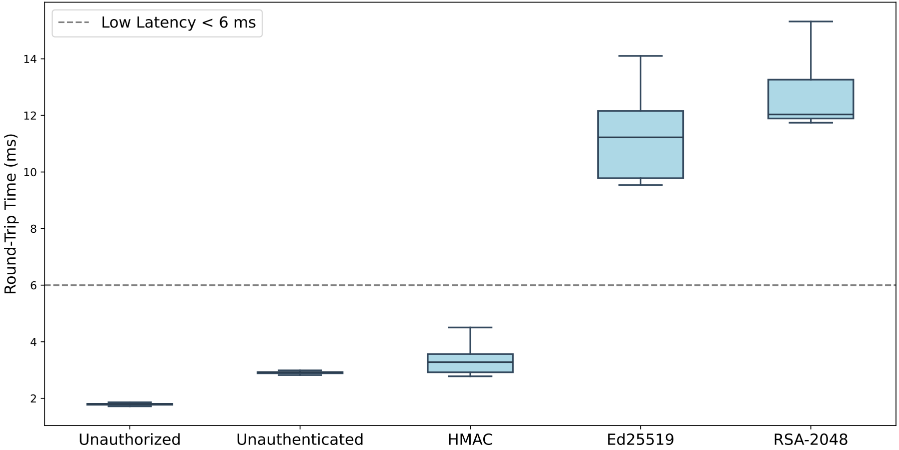
Integrity-Focused Attacks

- Message Creation
- Message Modification
- Message Replay
- Message Delay

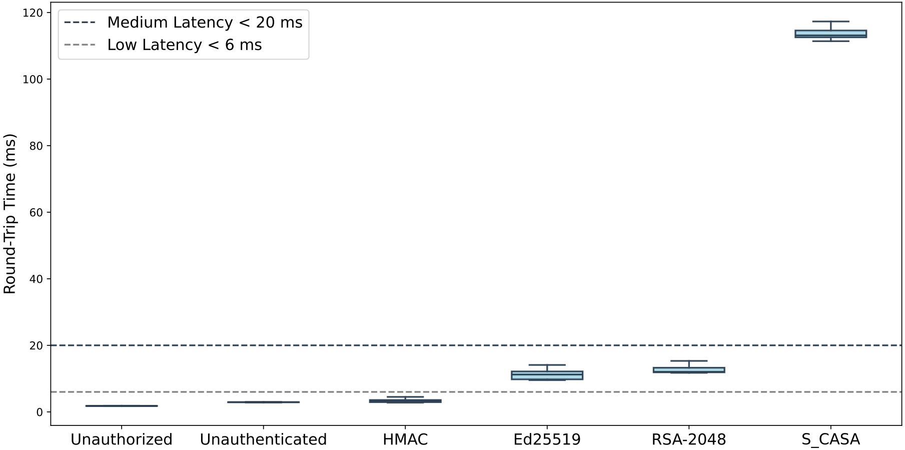
Authenticity-Focused Attacks

- Collusion
- Existential Unforgeability under Chosen-Message Attacks

Performance Analysis



Performance Analysis



Performance Analysis: S_{CASA}

Message Exchange Round-Trip Time

Minimum	Average	Maximum	Deviation
≈ 111 ms	≈ 120 ms	≈ 510 ms	≈ 29 ms

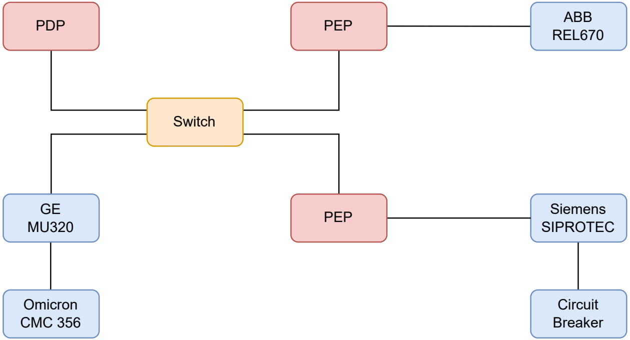
Speedup Solutions

- Optimization of implementation
- Hardware acceleration

Cryptography-Driven Authentication, Authorization, & Access Control

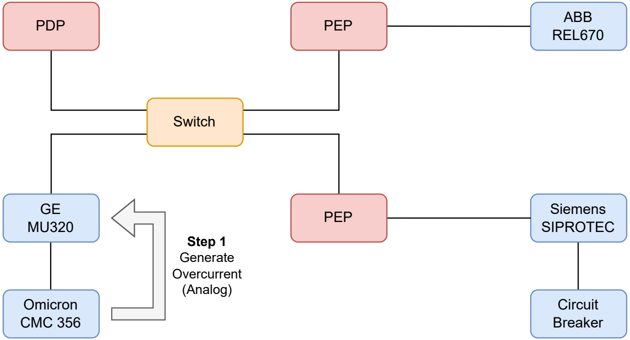
Authentication, authorization, & access control integrated into a single attribute-based PKC scheme
→ **Advantage:** Privacy & Anonymity

Compatibility Analysis



PDP. . . Policy Decision Point | PEP. . . Policy Enforcement Point

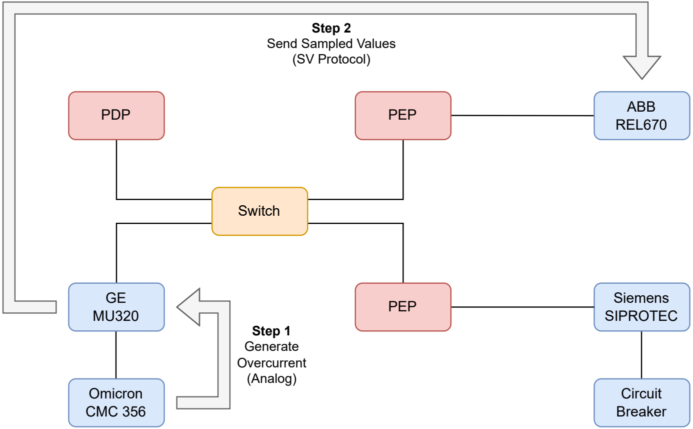
Compatibility Analysis



Step 1
Generate
Overcurrent
(Analog)

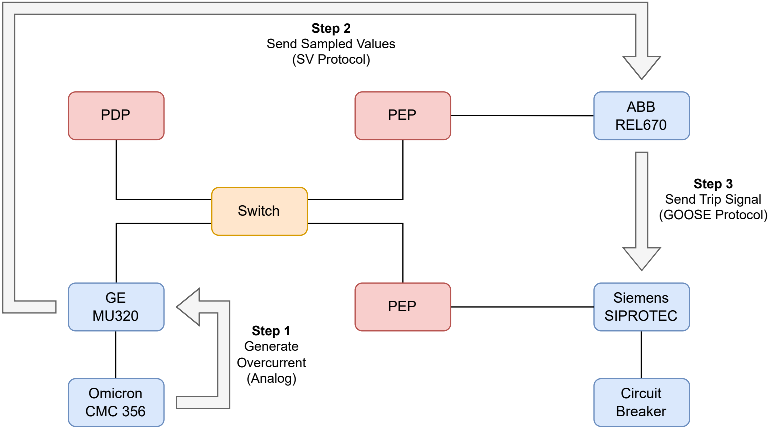
PDP. . . Policy Decision Point | PEP. . . Policy Enforcement Point

Compatibility Analysis



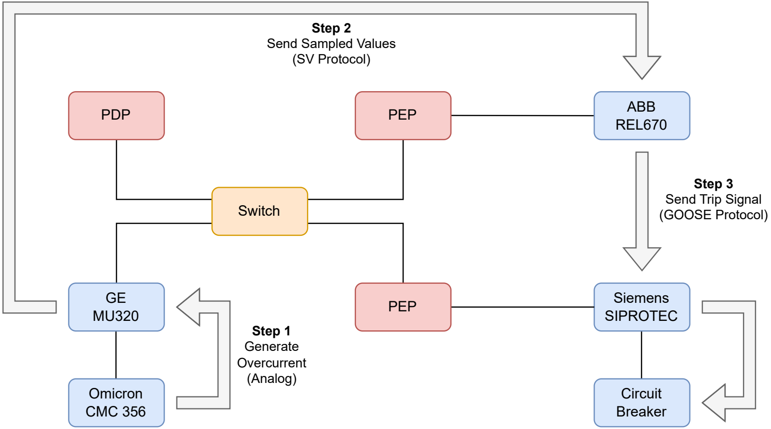
PDP. . . Policy Decision Point | PEP. . . Policy Enforcement Point

Compatibility Analysis



PDP. . . Policy Decision Point | PEP. . . Policy Enforcement Point

Compatibility Analysis



PDP. . . Policy Decision Point | PEP. . . Policy Enforcement Point

Future Work

AI for Policy Management

Integration of CASC-SAS with AI-based intrusion detection for security policy creation & modification
→ **Advantage:** Mitigation of a wider range of cyberattacks in a timelier manner

SDN-Based Realization

Aggregation of PEPs by deploying a virtual PEP for each port of a Software-Defined Networking (SDN) switch
→ **Advantage:** Reduced costs of deployment & reduced architectural complexity

Extended Demonstration of Applicability

Employment in time-critical systems with similar requirements & constraints
→ **Examples:** Industry 4.0, robotics, avionics, & medical systems

Conclusion

Problem

Expressive & flexible access control, & malleable PKC: Applicable to the SAS domain?
→ Constrained resources & communication time

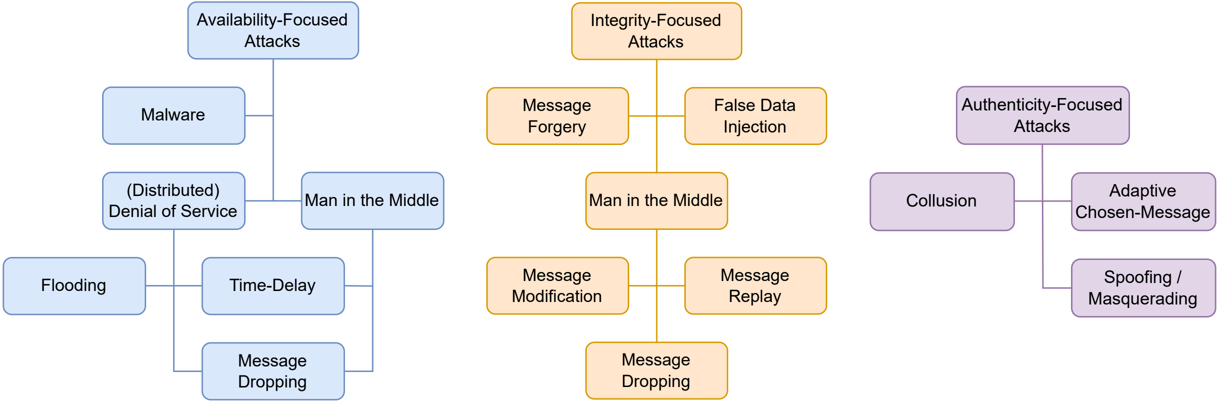
Contribution

CASC-SAS security architecture & framework. . .
. . . employs mandatory authentication, authorization, & access control
. . . for time-critical SAS communication
. . . in time-variable SAS environment.

Thank you!

Appendix

Adversarial Attacks


Availability-Focused Attacks

Malware

(Distributed) Denial of Service

Man in the Middle

Flooding

Time-Delay

Message Dropping

Integrity-Focused Attacks

Message Forgery

False Data Injection

Man in the Middle

Message Modification

Message Replay

Message Dropping

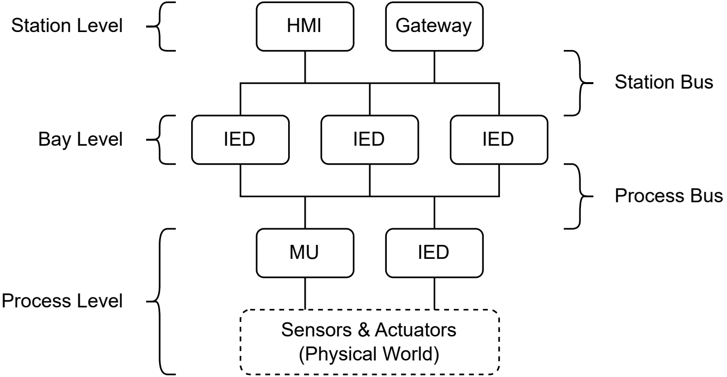
Authenticity-Focused Attacks

Collusion

Adaptive Chosen-Message

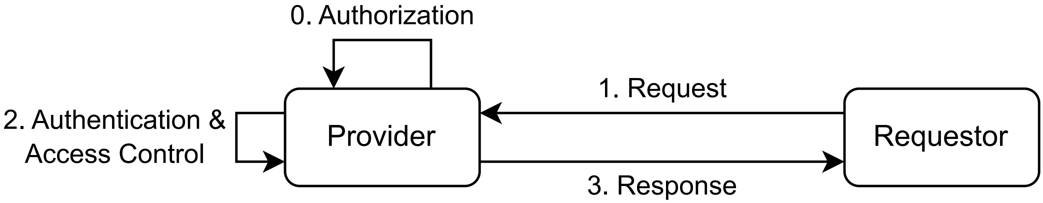
Spoofing / Masquerading

Substation Automation System (SAS)



IED. . . Intelligent Electronic Device | MU. . . Merging Unit | HMI. . . Human-Machine Interface

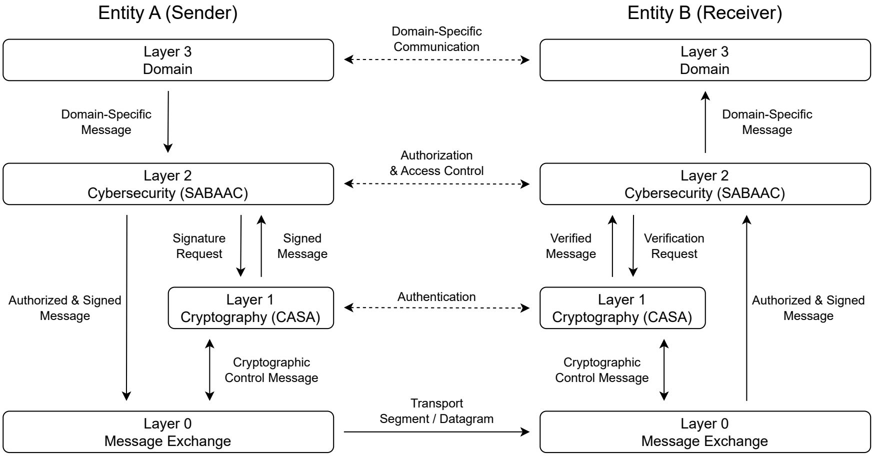
Authentication, Authorization, & Access Control



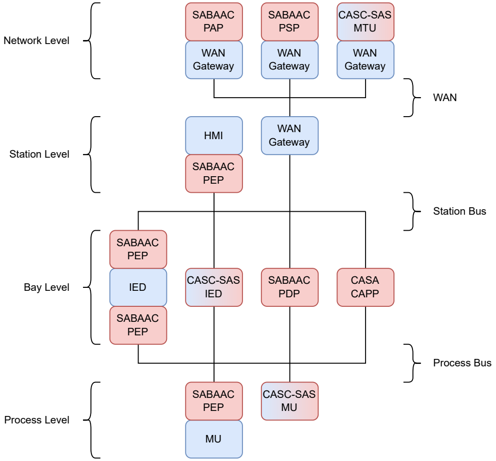
Problem

Too many provider responsibilities
→ Policy Management/Decisions/Enforcement, Request Verification, & Response Creation

CASC-SAS Architecture: Function-Oriented

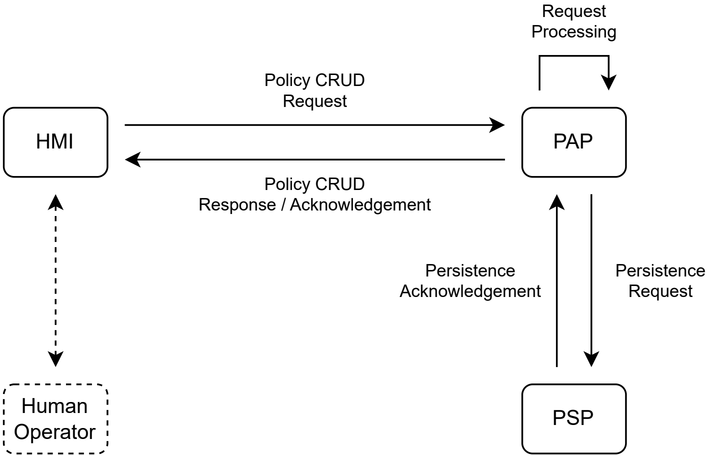


CASC-SAS Architecture: Component-Oriented

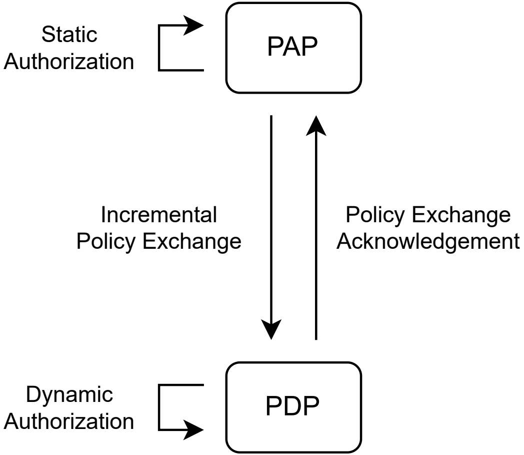


CAPP	CASA Administration & Processing Platform
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PSP	Policy Storage Point
HMI	Human-Machine Interface
IED	Intelligent Electronic Device
MTU	Master Terminal Unit
MU	Merging Unit
WAN	Wide Area Network

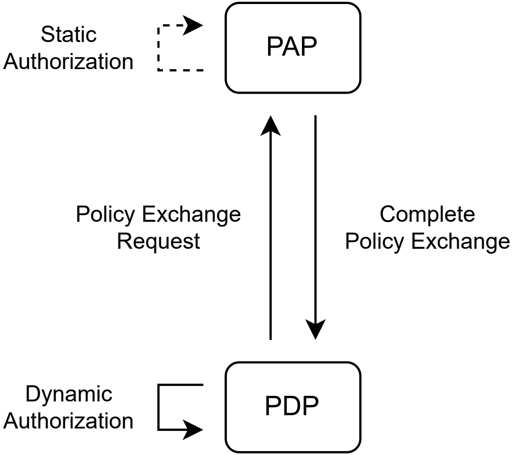
SABAAC: Static Authorization



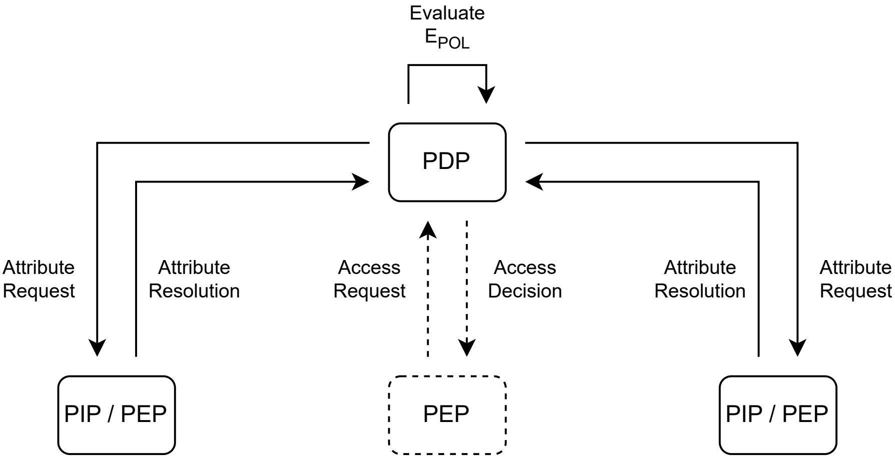
SABAAC: Policy Exchange Incremental



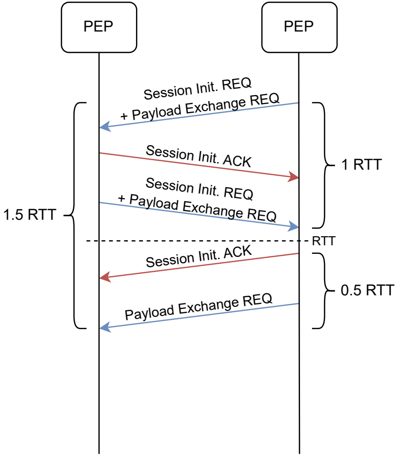
SABAAC: Policy Exchange Complete



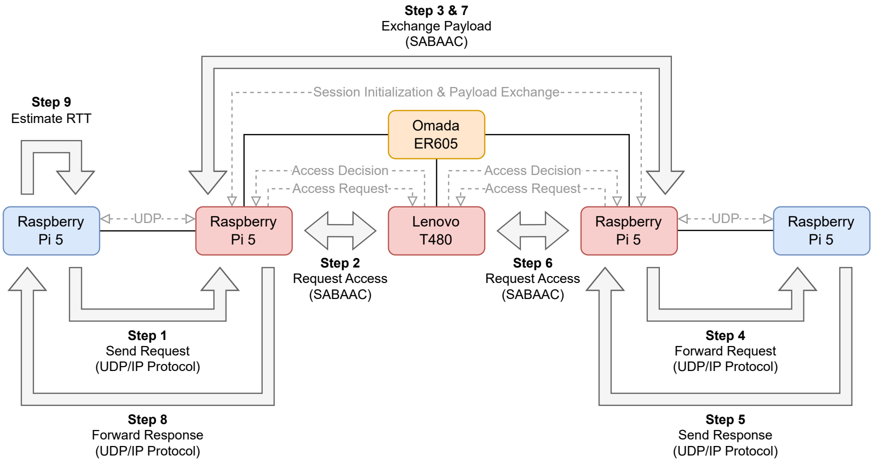
SABAAC: Dynamic Authorization



SABAAC: Session Initialization Piggybacking



Performance Evaluation: Sequence of Events



Related Work: ABAC

Attribute-Based Access Control (ABAC)

- T-ABAC: An attribute-based access control model for real-time availability in highly dynamic systems (Burmester et al. 2013)
- Firewall for Attribute-Based Access Control in Smart Grids (Ruland and Sassmannshausen 2018)
- An Attribute-Based Access Control for IoT Using Blockchain and Smart Contracts (Zaidi et al. 2021)
- A user-friendly attribute-based data access control scheme for smart grids (Mu et al. 2023)
- Accountable multi-authority attribute-based data access control in smart grids (Zhang et al. 2023)
- Secure Identities for Renewable Energy Sources Through Self-Sovereign Identity and Attribute-Based Access Control (Volkmann et al. 2024)

Paper: ABS-SAS

Concept

Attribute-based signature (ABS) scheme for substation automation systems (SAS)
→ **Authentication & authorization** via cryptographic scheme

Work Plan

Currently: Implementation in C++, & **evaluation** of the scheme with regard to security & performance aspects
Soon: Discussion of evaluation findings, **finalization** of paper, & **proofreading**

Submission (Planned)

Workshop @ 23rd International Conference on Applied Cryptography and Network Security (**ACNS**) in Munich

References I

[1] Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen. “Policy enforcement system for secure interoperable control in distributed Smart Grid systems”. In: *Journal of Network and Computer Applications* 59 (Jan. 2016), pp. 301–314. ISSN: 1084-8045. DOI: `10.1016/j.jnca.2015.05.023`.

[2] Mike Burmester, Emmanouil Magkos, and Vassilis Chrissikopoulos. “T-ABAC: An attribute-based access control model for real-time availability in highly dynamic systems”. In: *2013 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, July 2013. DOI: `10.1109/iscc.2013.6754936`.

[3] Ghada Elbez, Hubert B. Keller, and Veit Hagenmeyer. “Authentication of GOOSE Messages under Timing Constraints in IEC 61850 Substations”. In: *Electronic Workshops in Computing*. BCS Learning & Development, Sept. 2019. DOI: `10.14236/ewic/icscsr19.17`.

[4] Junho Hong et al. “Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations”. In: *IEEE Transactions on Industrial Informatics* 15.7 (July 2019), pp. 4332–4341. ISSN: 1941-0050. DOI: `10.1109/tii.2018.2884728`.

References II

[5] Vincent C. Hu et al. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. Tech. rep. NIST Special Publication 800-162. National Institute of Standards and Technology, Jan. 2014. DOI: 10.6028/nist.sp.800-162.

[6] International Electrotechnical Commission. “Part 5: Communication requirements for functions and device models”. In: *Communication networks and systems for power utility automation (IEC 61850)* (2014).

[7] International Electrotechnical Commission. “Part 6: Security for IEC 61850”. In: *Power systems management and associated information exchange - Data and communications security (IEC 62351)* (2020).

[8] International Electrotechnical Commission. “Part 8: Role-based access control for power system management”. In: *Power systems management and associated information exchange - Data and communications security (IEC 62351)* (2020).

References III

[9] International Electrotechnical Commission. “Part 81: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 95061 and ISO 95062) and to ISO/IEC 88023”. In: *Communication networks and systems for power utility automation (IEC 61850)* (2022).

[10] Dmitry Ishchenko and Reynaldo Nuqui. “Secure Communication of Intelligent Electronic Devices in Digital Substations”. In: *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*. IEEE, Apr. 2018. DOI: `10.1109/tdc.2018.8440438`.

[11] Byunghun Lee et al. “Role-based access control for substation automation systems using XACML”. In: *Information Systems* 53 (Oct. 2015), pp. 237–249. ISSN: 0306-4379. DOI: `10.1016/j.is.2015.01.007`.

[12] Mingchao Ma and Steve Woodhead. “Constraint-Enabled Distributed RBAC for Subscription-Based Remote Network Services”. In: *The Sixth IEEE International Conference on Computer and Information Technology (CIT’06)*. IEEE, 2006. DOI: `10.1109/cit.2006.63`.

References IV

[13] Tianshi Mu et al. “A user-friendly attribute-based data access control scheme for smart grids”. In: *Alexandria Engineering Journal* 67 (Mar. 2023), pp. 209–217. ISSN: 1110-0168. DOI: 10.1016/j.aej.2022.12.041.

[14] Mikel Rodriguez et al. “A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems”. In: *IEEE Access* 9 (2021), pp. 51646–51658. ISSN: 2169-3536. DOI: 10.1109/access.2021.3069088.

[15] Christoph Ruland and Jochen Sassmannshausen. “Firewall for Attribute-Based Access Control in Smart Grids”. In: *2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, Aug. 2018. DOI: 10.1109/sege.2018.8499306.

[16] Joint Task Force Interagency Working Group. *Security and Privacy Controls for Information Systems and Organizations*. Tech. rep. NIST Special Publication 800-53,Rev.5. National Institute of Standards and Technology, Sept. 2020. DOI: 10.6028/nist.sp.800-53r5.

References V

[17] Moritz Volkmann et al. “Secure Identities for Renewable Energy Sources Through Self-Sovereign Identity and Attribute-Based Access Control”. In: *13th International Conference on Renewable Energy Research and Applications (ICRERA)*. IEEE, Nov. 2024, pp. 394–399. DOI: `10.1109/icrera62673.2024.10815352`.

[18] Syed Yawar Abbas Zaidi et al. “An Attribute-Based Access Control for IoT Using Blockchain and Smart Contracts”. In: *Sustainability* 13.19 (Sept. 2021), p. 10556. ISSN: 2071-1050. DOI: `10.3390/su131910556`.

[19] Leyou Zhang et al. “Accountable multi-authority attribute-based data access control in smart grids”. In: *Journal of King Saud University - Computer and Information Sciences* 35.7 (July 2023), p. 101597. ISSN: 1319-1578. DOI: `10.1016/j.jksuci.2023.101597`.