Karlsruhe Institute of Technology

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

Master's Thesis Mid-Term Presentation

Moritz Gstuer | 31. October 2024

Agenda

1. Motivation

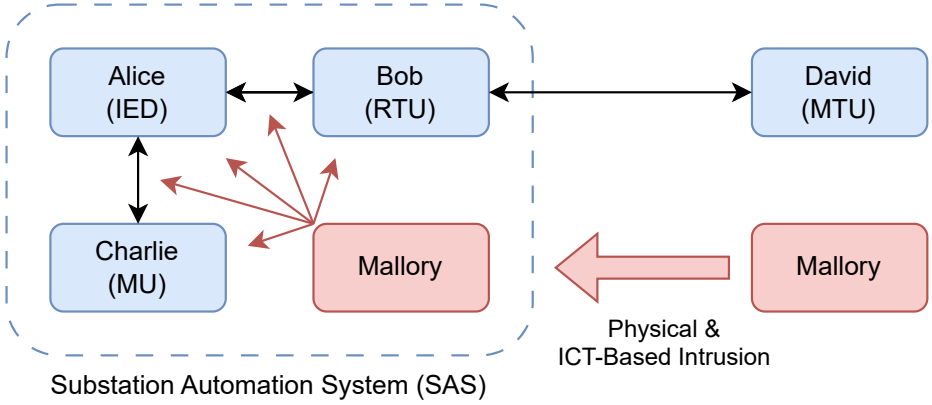
2. Approach

3. Work Plan

4. Evaluation

5. Conclusion

Motivation



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

SAS Communication: Requirements & Constraints

Requirements

- Integrity
- Authenticity
- Non-Repudiation
- Least Privilege Principle (PoLP)
- Separation of Duties (SoD)

→ Authentication, 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)

Research Questions

Authorization & Access Control in SAS

How can expressive and flexible but yet computationally expensive access control be employed in a SAS?
→ Real-Time Attributes, Ad-Hoc Policy Evaluation, & Speedup Solutions

Public-Key Cryptography in SAS

How can a secure and lightweight public-key approach be designed, implemented, & employed in a SAS?
→ (Dis-)Advantages, & Speedup Solutions

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?
→ System Model, Domain Requirements, Architecture, & Protocols

CASC-SAS Approach

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

- **S**erver-Aided **A**ttribute-**B**ased **A**uthorization & **A**ccess **C**ontrol (SABAAC)
- **C**ertificateless **A**ttribute-Based **S**erver-Aided **A**uthentication (CASA)

Authentication, Authorization, & Access Control

Problem: Policy Evaluation Complexity

Fine-grained & flexible access control relying on dynamic authorization & authentication
→ Ad-hoc evaluation in real-time environment

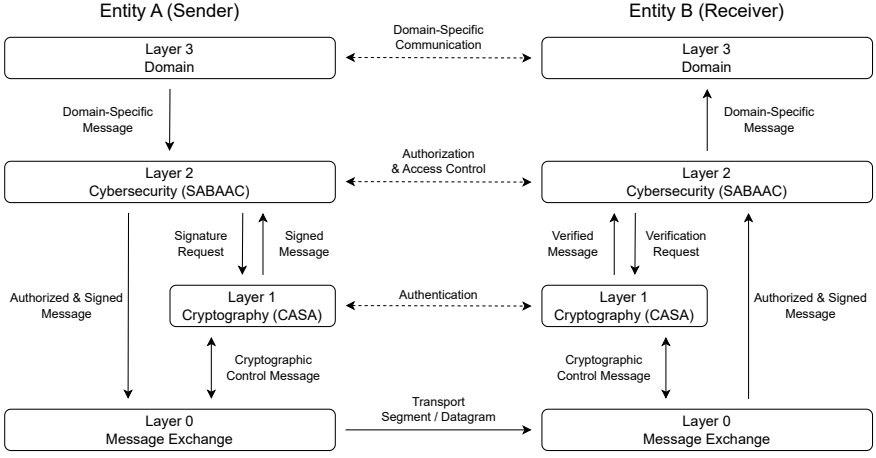
Solution: Server-Aided Access Control

Delegation of authorization & access control to semi-trusted server (PDP)
→ Authentication at each device (server-aided)
→ Speedup Techniques: Evaluation pre-computation & access decision caching

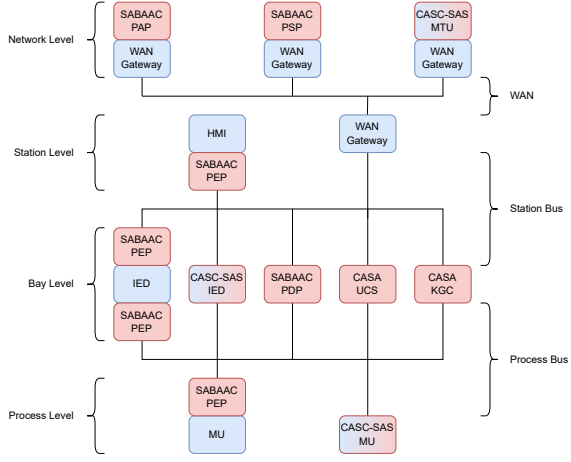
Architecture (Hu et al. 2014; OASIS Open 2013)

- Policy Decision Point (PDP) → Computes access decisions by evaluating policies
- Policy Enforcement Point (PEP) → Enforces policy decisions by controlling access to protected objects

CASC-SAS Architecture: Function-Oriented



CASC-SAS Architecture: Component-Oriented



HMI... Human-Machine Interface
IED... Intelligent Electronic Device
KGC... Key Generation Center
MTU... Master Terminal Unit
MU... Merging Unit
PAP... Policy Administration Point
PDP... Policy Decision Point
PEP... Policy Enforcement Point
PSP... Policy Storage Point
RTU... Remote Terminal Unit
UCS... Untrusted Cryptography Server
WAN... Wide Area Network

Work in Progress

Milestone: Realization

Finished: Local authentication, delegated authorization, & delegated access control protocol
In Progress: Server-aided authentication via own signature scheme, & policy DSL
→ Currently: ∼3100 SLOC, object-oriented, Java 17 & Kotlin
→ Planned: ∼5000 SLOC, published open-source

Milestone: Evaluation

Finished: Testbed construction & preliminary performance results
In Progress: Evaluation of performance, security, & compatibility
→ Planned: Code & results of experiments published open-source

What's next?

Milestone: Conclusion

Limitations, future work, & summary of thesis

Milestone: Review & Finalization

Thesis: Proofreading, review, printing, & binding
Final Presentation: Preparation, proofreading, & review

Estimated Time of Completion (ETC)

Draft: November 25, 2024
Final: January 01, 2025
Deadline: February 03, 2025

Performance Evaluation

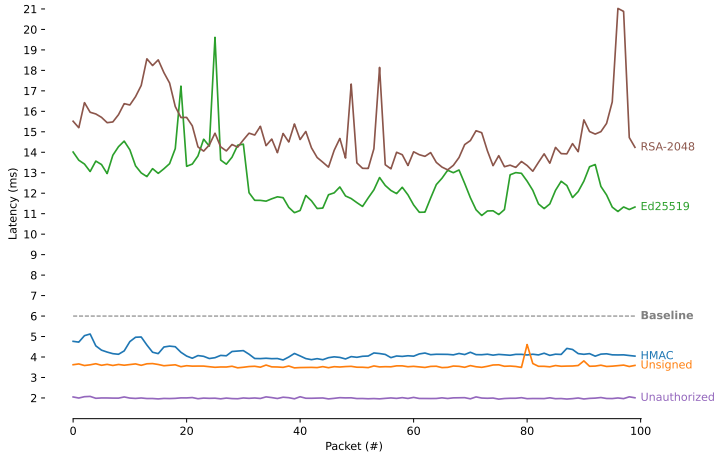
Question

Is CASC-SAS capable of securing time-constrained communication of a SAS?
→ Computational complexity, supported message types, & network exception resilience

Approach

Experimentally performed evaluation based on realization
→ Currently: Testbed-based experiments
→ Planned: Lab-based experiments

Preliminary Results



Discussion: 10k Sequential Packets

Access Control Overhead

	Avg	Min	Throughput
Unauthorized	2.0 ms	1.7 ms	465 PPS
Unsigned	3.3 ms	2.8 ms	292 PPS

→ Access Control: +1.3 ms RTT (+65 %)

Authentication Overhead

	Avg	Min	Throughput
HMAC	3.4 ms	2.9 ms	285 PPS
Ed25519	12.0 ms	9.6 ms	82 PPS
RSA-2048	14.0 ms	11.4 ms	68 PPS

→ Authentication: +0.1–10.7 ms RTT (+3–325 %)

Conclusion

Problem

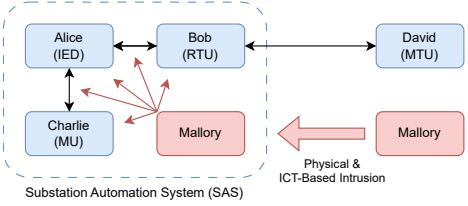
Current IT cyberattack mitigation approaches: Not applicable to the SAS domain!
$\rightarrow$ Constraints: Resources, time, & communication patterns

Contribution

CASC-SAS Security Architecture & Framework...
... employs mandatory authentication, authorization, & access control
... for time-critical SAS communication
... in time-variable SAS environment.

Thank you!

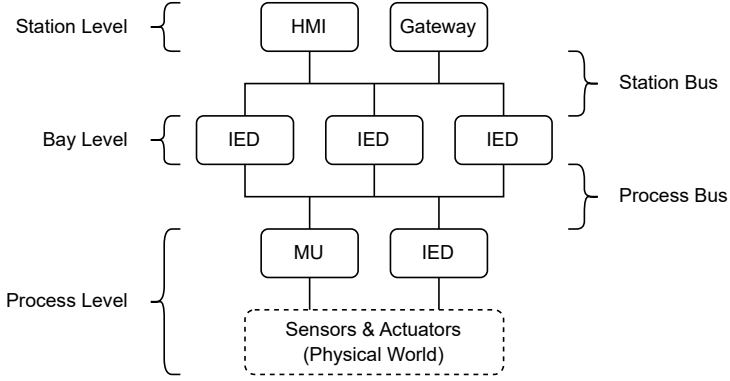
Motivation



Substation Threats & Attacks

- Eavesdropping
- Man-in-the-Middle
- Spoofing/Masquerading
- Replay
- Denial of Service
  → Flooding, Broadcast/Multicast Storm, & Poisoning
- False Data Injection
  → Forged Sensor Data & Commands, & Configuration Tampering

System Model: Substation Automation System (SAS)



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

Related Work

IEC 62351 (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)

Role-Based Access Control (RBAC) in Substations

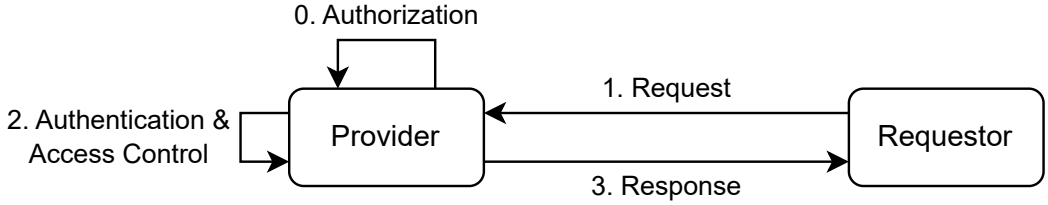
- XACML-Based RBAC Approach for IEC 61850 & IEC 62351 compliant SAS (Lee et al. 2015)
- Distributed RBAC for Subscription-Based Remote Network Services (Ma and Woodhead 2006)
- Rule-Based RBAC Policy Enforcement Architecture (Alcaraz, Lopez, and Wolthusen 2016)

Related Work

Attribute-Based Access Control (ABAC) in Substations

- Firewall for Attribute-Based Access Control in Smart Grids (Ruland and Sassmannshausen 2018)
  - → Firewall with XACML-Based ABAC Policies
  - → Outer & Inner Station Bus
  - → Unobstructed Fast Messages (e.g. GOOSE)
- T-ABAC: An attribute-based access control model for real-time availability in highly dynamic systems (Burmester, Magkos, and Chrissikopoulos 2013)
  - → Real-Time Attribute Values
  - → Labeling of High Priority Packets
  - → Domain-Based Congestion Avoidance

Traditional Authorization, Authentication, & Access Control



Problem

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

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.

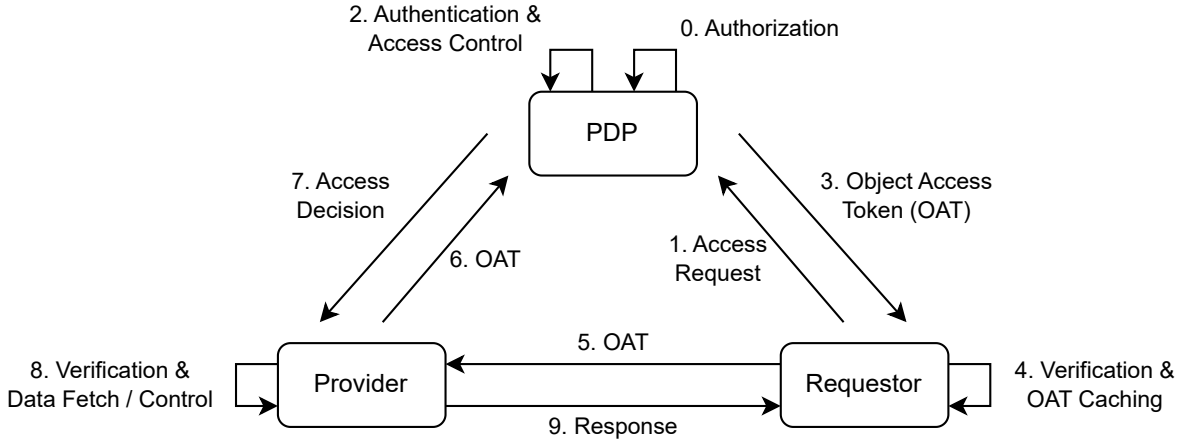
Discussion (Hu et al. 2014)

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

Architecture (Hu et al. 2014; OASIS Open 2013)

- Policy Decision Point (PDP) → Computes access decisions by evaluating policies
- Policy Enforcement Point (PEP) → Enforces policy decisions by controlling access to protected objects

Server-Aided ABAC



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] 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.

[4] 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.

References II

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

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

[7] 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).

[8] 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).

References III

[9] 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.

[10] 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.

[11] 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.

[12] OASIS Open. *eXtensible Access Control Markup Language (XACML) Version 3.0*. 2013. URL: https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf (visited on 05/06/2024).

References IV

[13] 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.

[14] 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.

[15] 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.