Karlsruhe Institute of Technology

KASTEL

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

Master's Thesis Short Proposal of

Moritz Gstür

At the KIT Department of Informatics
Institute for Automation and Applied Informatics (IAI)

First examiner:	Prof. Dr. Veit Hagenmeyer
Second examiner:	TBD
First advisor:	Dr. Mohammed Ramadan
Second advisor:	Dr.-Ing. Ghada Elbez

15. April 2024 – 05. August 2024

I declare that I have developed and written the enclosed thesis completely by myself. I have not used any other than the aids that I have mentioned. I have marked all parts of the thesis that I have included from referenced literature, either in their original wording or paraphrasing their contents. I have followed the by-laws to implement scientific integrity at KIT.

Karlsruhe, 05. August 2024

. . . . . .

(Moritz Gstür)

Abstract

Substation automation systems (SAS) increasingly rely on information and communication technology for monitoring and control. This leads to new challenges with regard to information security. Existing standards such as IEC 61850 and IEC 62351 do not sufficiently cover recent developments, including attribute-based access control (ABAC) and attribute-based public key cryptography (AB-PKC). Therefore, we propose a certificateless attribute-based server-aided cryptosystem for SAS (CASC-SAS). Our approach consists of two core concepts referred to as CASA and SABAAC. The certificateless attribute-based server-aided authentication (CASA) provides asymmetric cryptographic protocols and schemes that serve as a foundation for cybersecurity approaches in a SAS. The server-aided attribute-based authorization and access control (SABAAC) prevents unauthorized access to devices of a SAS based on ABAC policies. By employing server-aided protocols and speedup techniques, our approach takes the strict time and resource constraints of the SAS domain into account. To demonstrate our approach, we propose realizing it as a fully functional test bed that mimics the behavior of a real interconnected SAS. Moreover, we propose a theoretical and experimental evaluation of the security, performance, and compatibility aspects of our approach.

Contents

List of Figures

1. Introduction

Modern Operational Technology (OT) such as Industrial Control Systems (ICS) increasingly rely on Information and Communication Technology (ICT) for monitoring and control [1]. As a consequence, the resemblance of OT and Information Technology (IT) systems increases, as OT systems adopt IT technology. This development leads to new possibilities including the integration of distributed OT into Supervisory Control And Data Acquisition (SCADA) systems. Nevertheless, new challenges arise from the increased usage of ICT in OT systems.

According to Stouffer et al. [1], the typical long life cycle of OT systems and their unique requirements regarding performance, reliability, security, safety, privacy, and environmental impact have to be taken into account when designing, operating, and maintaining OT systems. In the following, we focus on the information security of OT systems. Although a variety of information security solutions exist for IT, migration of existing approaches to the OT domain may not be a viable solution due to the differing system characteristics, risks, and priorities. An example for the differing priorities are information confidentiality and access control. While the prevention of unauthorized access represents the core objective of IT security approaches, OT systems and especially OT-based critical infrastructures prioritize system availability and reliability.

Within the scope of this thesis, we focus on the occurring communication in a specific type of OT system. The field of application of the approach proposed by this thesis is known as Substation Automation System (SAS). A SAS represents the entirety of communication and control equipment of a substation [2]. A substation is a facility of a high-voltage electricity grid connecting power transmission and distribution lines that use different voltage levels [3]. A substation and its SAS represent a specific type of ICS. The tasks of a SAS are time-critical and have to be executed reliably, as the electricity sector and its substations are critical infrastructures.

The IEC 61850 series provides standards for the communication networks of digital energy systems [4]. The goal of the IEC 61850 series is seamless communication and interoperability of systems in a smart energy grid. Although standards for the communication in a SAS are provided by the IEC 61850 standards, information security is not an objective of these standards. To overcome this problem, the IEC 62351 standard series was created by the International Electrotechnical Commission. Part 6 of the IEC 62351 series provides standardized security means for communication compliant to IEC 61850 [5]. Moreover, Part 8 of the IEC 62351 series provides a role-based access control concept for power system [6].

1.1. Objective

Although standards regarding the communication networks of smart grid systems are widely accepted and utilized, information security continues to confront unresolved challenges. Historical evidence indicates that economically or politically motivated adversaries pose a risk to OT systems, including energy-related systems. The Communications Security Establishment Canada [7] published a list of 28 OT-related cybersecurity incidents between 2010 and 2020, including incidents in energy-related sectors. These incidents comprise 13 state-sponsored incidents, 13 cybercrime incidents, and two incidents perpetrated by thrill-seeking individuals. The state-sponsored incidents include the Stuxnet malware deployed in Iranian nuclear power and enrichment facilities in 2010 [8], the Shamoon malware used against Saudi Aramco in 2012 [9], the Blackenergy malware used to attack Ukrainian power distribution systems in 2015 [10], the Industroyer/CrashOverride malware used to shut down remote terminal units of a Ukrainian power transmission facility in 2016 [11, 12], and the Triton/Trisis malware used to attack Triconex Safety Instrumented System (SIS) controllers in 2017 [13].

Despite the existence of standards for communication and information security including the IEC 61850 and 62351, there are remaining challenges in order to secure SAS communication. This thesis focuses on these remaining challenges to enhance the information security of SAS communication. As stated by Ishchenko and Nuqui [14], these challenges include, among others, ensuring the integrity and authenticity of substation control and protection communication without compromising the time criticality. For this purpose, cryptographic signature and verification approaches can be employed in the SAS environment. According to Elbez et al. [15], the strict time constraints of the low latency communication in substations are key factors for the information security. Accordingly, Public Key Cryptography (PKC) formerly specified by the IEC 62351 standards is not appropriate due to computational complexity and latency.

Due to an increase in processing performance of IT and OT devices nowadays, this thesis examines the applicability of effective and efficient PKC in substations. For this purpose, this thesis proposes new cryptographic and cybersecurity approaches for authentication, authorization, and access control. Moreover, the thesis discusses the employment of speedup techniques to enable the usage of secure PKC in time-critical OT systems. Therefore, the following research questions are going to be answered in the course of this thesis:

RQ1 How can expressive and flexible but yet computationally expensive access control approaches such as Attribute-Based Access Control (ABAC) be employed to enable prevention of unauthorized access, enable the Separation of Duties (SoD), and ensure the Principle of Least Privilege (PoLP) in a time-critical SAS environment?

RQ2 How can a secure and lightweight PKC approach be designed and implemented, that is able to ensure the authenticity, integrity, and non-repudiation of communication in a time-critical SAS environment?

RQ3 How can authentication, authorization, and access control be integrated into a malleable, scalable, and lightweight cryptosystem for time-critical SAS communication?

1.2. Contribution

With the aim of providing means to enhance the information security in a SAS, we propose a **C**ertificateless **A**ttribute-Based **S**erver-Aided **C**ryptosystem for **S**ubstation **A**utomation **S**ystems (CASC-SAS). The main objective of the proposed approach is to provide secure protocols, algorithms, and schemes for SAS communication based on asymmetric cryptography. The provided protocols, algorithms, and schemes aim to satisfy SAS security requirements such as integrity, authenticity, access control, and non-repudiation. Furthermore, the approach takes the specific characteristics, risks, and priorities of OT, ICS, and SAS into account. To address the aforementioned objectives and considerations, this thesis comprises the following contributions:

- Identification of security, safety, availability, performance, and compatibility requirements of the proposed approach, and development of a system model, which represents the corresponding field of application.
- Design of a server-aided attribute-based authorization and access control approach called SABAAC, which relies on speedup techniques such as access decision caching and policy evaluation precomputation.
- Design of a certificateless attribute-based public key cryptography approach for digital signatures called CASA, which features server-aided verification and online/offline cryptography.
- Design of a certificateless attribute-based server-aided cryptosystem for SAS called CASC-SAS, which integrates SABAAC and CASA into a dual-path four-layered system architecture.
- Implementation of the proposed approach using high-level programming languages, and deployment of the implementation to a fully functional test bed that mimics the behavior of an interconnected OT system.
- Security evaluation to proof the security characteristics of the approach.
- Performance evaluation to demonstrate the applicability of the approach in an OT environment with strict time and resource constraints.
- Compatibility evaluation to demonstrate the feasibility of the approach for the construction and retrofitting of a SAS.

2. Fundamentals

The purpose of this chapter is to introduce, define, and describe the fundamental terms and concepts of this thesis proposal. This chapter provides an introduction for access control in section 2.1. Moreover, the relevant fundamentals of cryptography are discussed in section 2.2.

2.1. Attribute-Based Access Control

Access control is the process of granting and denying specific requests to logical or physical services and resources [16]. Based on the type of service or resource guarded by the access control, two types of access control can be distinguished. Physical access control supervises access requests to physical facilities. Logical access control supervises the access to information and information processing services. Within the scope of the thesis proposal, the term access control will be used to describe logical access control for IT and OT systems.

Logical access control protects objects like data, services, executable applications, or network devices from unauthorized operations [17]. An operation is performed by a subject on a specific object. To protect an object, its owners establish access control policies. These policies describe which subjects may perform certain operations on a specific object. The policies are enforced by a logical component referred to as Access Control Mechanism (ACM) [17]. The ACM receives the access request from a subject, decides whether the request should be granted or denied, and enforces the decision taken. The ACM takes the decision based on a framework called access control model. The access control model defines the functionalities and environment including subjects, objects, and rules for the ACM to take and enforce a decision.

Attribute-Based Access Control (ABAC) is an access control model enabling access decisions based on attributes associated with subjects, objects, actions, and the environment of a system [18]. In other words, in ABAC an access request of a subject to perform operations on an object is decided based on assigned attributes of the subject and object, environment conditions, and a set of policies [17]. Within the context of ABAC, an attribute is a characteristic containing information in the form of a name-value pair [17]. A subject attribute such as identity, clearance, or department describes the characteristics of a person or non-person entity. An object attribute such as the object classification, type, or owner describes the resource for which the access is requested. An operation or action attribute describes the function performed on an object by a subject. The environment conditions or

environment attributes describe the context of an access request. Environment conditions include dynamic characteristics like time of the day, day of the week, and request location of the subject.

A policy represents a rule based on which an access decision is taken for specific attributes [17]. As a consequence, a policy can be seen as a relationship between subject, object, environment, and operation attributes describing under which circumstances the ACM grants or denies an access request.

Role-Based Access Control (RBAC) and Identity-Based Access Control (IBAC) represent special cases of ABAC regarding their attributes used [17]. An advantage of ABAC compared to other access control models is the higher flexibility regarding multifactor policy expression. Moreover, ABAC can take access control decisions based on ad-hoc knowledge and knowledge from separate infrastructure. This is possible due to ABAC taking decisions at request time by evaluating policies instead of static decision-making as found in IBAC and RBAC.

2.2. Public Key Cryptography

Cryptography is a scientific discipline concerned with the study of methodologies, algorithms, schemes, and protocols for the encryption and verification of information [19, 20, 21]. In other words, cryptography provides means to prevent unauthorized access and to enable the verification of information. The objective of cryptography is to satisfy specific security goals, including the assurance of confidentiality, integrity, authenticity, and non-repudiation.

A cryptographic system or cryptosystem is a set of cryptographic algorithms [22]. A cryptosystem comprises sets of valid inputs and outputs as well as required cryptographic keys [23]. Two important principles for the design of cryptosystems were formulated by Kerckhoffs and Shannon. As stated by Kerckhoffs, the cryptosystem must not require secrecy and must be able to be known by the adversary without inconvenience [24]. According to Shannon, it shall be assumed that the adversary knows the system being used [25]. The goal of a cryptosystem is to provide specific cryptographic services such as encryption or verification. Verification describes the process of proving the integrity, authenticity, or non-repudiation of information [26]. The verification of information is based on a so-called tag or signature created by a signature algorithm. Encryption describes the process of transforming plain information called plaintext into an unintelligible form called ciphertext to maintain its secrecy [19, 26]. The inverse process of encryption is referred to as decryption.

Public Key Cryptography (PKC), also referred to as asymmetric cryptography, relies on algorithms which use a pair of two related keys for a cryptographic operation and its inverse operation [20, 21, 23]. The pair of related keys in PKC consists of a private key, which must be kept secret, and a public key, which may be shared without consequences for security, as long as its authenticity and integrity is ensured. In contrast to PKC, secret-key or symmetric cryptography uses the same key for a cryptographic operation and its inverse operation.

PKC offers the following advantages over symmetric cryptography [20, 23]: Firstly, PKC does not require a secure channel or secure protocol to exchange keys. Secondly, the overall number of required keys using PKC is lower. Moreover, the number of keys scales linear with the number of communication entities. For example in a network with n entities, n key pairs or $2n$ keys have to be established. In the same network, pairwise symmetric cryptography would require $n(n-1)/2$ keys.

Nevertheless, symmetric cryptography has advantages in comparison with asymmetric cryptography [20]. Firstly, symmetric-key algorithms are faster than asymmetric-key algorithms. Secondly, for a given level of security, symmetric cryptographic keys are shorter. This reduces the memory and bandwidth requirements for key storage and transmission.

2.2.1. Certificateless Public Key Cryptography

Certificateless Public Key Cryptography (CL-PKC) can be seen as an intermediate approach between Identity-Based Public Key Cryptography (ID-PKC) and certificate-based PKC approaches such as Public Key Infrastructure (PKI) [27]. CL-PKC approaches make use of a Trusted Third Party (TTP) called Key Generating Center (KGC) to generate partial private keys based on an entity's identity and a master key. To obtain the private key, the entity combines the partial private key with a secret value. Consequently, CL-PKC neither suffers from the key escrow problem nor requires a secure communication channel for the key distribution. To obtain the public key, the entity generates it based on public parameters and the secret value. Similar to ID-PKC, the public key is not derived from the private key and may therefore exist prior to it. The only restriction is that the public key and the private key must use the same secret value.

2.2.2. Attribute-Based Public Key Cryptography

Attribute-Based Public Key Cryptography (AB-PKC) is a generalization of the ID-PKC concept [28, 29, 30]. Attribute-Based Encryption (ABE) combines the principles of ABAC with the concept of PKC. Therefor, attribute-based policies are integrated into cryptographic algorithms in the form of access structures and attributes. ABE approaches are classified as either Key-Policy ABE (KP-ABE) or Ciphertext-Policy ABE (CP-ABE), depending on whether the access structure is associated with a key or a ciphertext [29, 31, 30]. In KP-ABE a secret key is able to decrypt a ciphertext if the attributes of the ciphertext satisfy the key-associated access structure. Consequently, a data owner cannot control who is able to access the data and has to trust a TTP to issue appropriate keys [31]. In CP-ABE a secret key is able to decrypt a ciphertext if the key-associated attributes satisfy the ciphertext's access structure. Accordingly, each data owner manages the access control policies for its own data, which makes CP-ABE more flexible and scalable than KP-ABE. Similar to the concept of ABE, Attribute-Based Signatures (ABS) enable the integration of attributes into signing and verification algorithms [32, 33].

3. Related Work

An authenticated communication approach for network packets between IEDs and merging units is presented by Ishchenko and Nuqui [14]. They introduce a system and bump-in-the-wire device called security filter as an add-on device between IEDs and Ethernet-based communication busses using the Generic Object Oriented Substation Event (GOOSE) or Sampled Values (SV) protocol. Security filter appends Message Authentication Code (MAC) tags to outgoing messages of the IEDs and verifies incoming MAC tags. As a consequence, the communication busses are secured against unauthenticated messages achieving the security goals integrity and authenticity. The authors showed that the security filter is able to meet the IEC 61850 performance requirements of GOOSE and SV [4] using a HMAC and GMAC algorithm even on commodity of-the-shelf ARM hardware.

A review of IEC 62351 security recommendations with regard to message authentication and a comparison of viable authentication approaches for IEC 61850 substations is presented by Elbez et al. [15]. The authors implemented a digital signature authentication scheme and a keyed Hash Message Authentication Code (HMAC) scheme for GOOSE messages and compared the required computational times. According to the authors, the computational times show that asymmetric cryptography solutions based on RSA and RSASSA-PSS are not suitable for the timing constraints of GOOSE messages. In contrast, the authentication time of the HMAC approach is of the order of microseconds, making it a more viable approach for the substation domain.

An authentication and encryption approach for substation communication using the protocols GOOSE and SV is presented by Rodriguez et al. [34]. The authors present a hardware architecture for the encryption and authentication of GOOSE and SV packets at wire-speed conforming to IEC 62351:2020 [5]. The hardware implementation is able to process GOOSE and SV packets with a fixed latency in the order of microseconds. Consequently, the authors state that the presented hardware architecture is able to provide integrity and confidentiality without exceeding the maximum delivery time of three milliseconds introduced by IEC 61850 for GOOSE and SV packets [4].

To protect substations against attacks, Hong et al. [35] present a domain-based collaborative mitigation approach. According to the authors, the goal of the approach is to enable substation devices to collaboratively defend against attacks. The authors present three attack scenarios that can be mitigated using the presented domain-based collaborative approach. The presented attack scenarios are an accidental or malicious IED configuration change, false sensor data injection, and false device command injection. Collaborating devices can block these attacks by validating sensor data and configuration changes based on measurements and metrics as well as predicting consequences of control actions.

An access control approach driven by ABAC policies for smart grid systems including substations is presented by Ruland and Sassmannshausen [36]. The presented access control approach is realized in the form of an access control firewall. The access control firewall splits the station bus into an inner and an outer region and connects these regions by processing access requests of connected devices. The inner station bus connects IEDs and enables low-latency GOOSE or GSSE communication between them. The access control firewall enforces access request decisions based on ABAC policies.

A real-time capable ABAC approach is presented by Burmester et al. [37]. The authors propose an extended ABAC model that is based on time-dependent attributes to support availability within the strict time constraints of cyber-physical systems. The availability of a time-dependent attribute can be expressed with an availability label that is dynamically determined based on user and system events as well as the context of the requested service. The authors demonstrate the real-time ABAC approach for IP multicast in Trusted Computing (TC) compliant networks.

An IEC 61850 and IEC 62351 compliant RBAC approach for substations is presented by Lee et al. [38]. The approach focuses on session-based access control for TCP/IP communication on the station bus of substations. The presented implementation relies on a role-based client-server architecture. The implementation demonstrates the feasibility of RBAC for substations as specified by IEC 62351 [6]. Furthermore, the presented implementation is capable of processing and responding to MMS requests within the 500 millisecond time requirement for type 3 messages (low speed messages) specified by IEC 61850-5 [4].

A distributed RBAC approach for subscription-based remote network services is presented by Ma and Woodhead [40, 39]. The authors propose a distributed authentication and role-based authorization framework called Distributed Role-based Access Control (DRBAC). The distributed authentication is realized by delegating the authentication of users to their subscribing institutions by issuing authentication delegation certificates. The role-based authorization approach extends traditional RBAC by adding the concept of distributed roles shared by the service provider and service subscribers. This enables access control policies associated with distributed roles rather than subject identities, which leads to an increase in scalability and manageability of access control. Moreover, the authors state that their DRBAC approach supports temporal, contextual, or cardinality constraints to enhance the semantic expressiveness of access control and enable the definition of higher-level organizational policies.

A rule-based RBAC policy enforcement approach for smart grid systems is presented by Alcaraz et al. [41]. The presented approach integrates into a smart grid system with supernode networking architecture. Supernodes are servers at fixed locations responsible for handling data flows of a set of subscribers [42]. The policy enforcement approach presented by Alcaraz et al. consists of three execution phases, namely authentication, authorization, and interoperability. The approach is based on a rule-based expert system and a context manager for the analysis of the subject, target object, and context of a request.

4. Approach

In the following section, we introduce our proposed security approach for substation automation systems. With the aim of securing the time-critical communication between resource-constrained devices in a time-variable environment, we propose a **C**ertificateless **A**ttribute-Based **S**erver-Aided **C**ryptosystem for **S**ubstation **A**utomation **S**ystems (CASC-SAS). The CASC-SAS cryptography and cybersecurity approach is able to prevent and mitigate cyberattacks by providing security schemes and mechanisms, and enforcing mandatory communication policies.

The goal of the approach is the enhancement of SAS security by providing secure authentication, authorization, and attribute-based access control for time-critical SAS communication. The CASC-SAS approach comprises two core concepts. The first core concept of the approach is the Certificateless Attribute-Based Server-Aided Authentication (CASA), which is further discussed in section 4.2. The second core concept of the approach is the Server-Aided Attribute-Based Authorization and Access Control (SABAAC), which is further discussed in section 4.3. Moreover, the approach is based on a dual-path four-layered architecture. The two paths are referred to as data path and control path. The four layers of the architecture are referred to as domain, cybersecurity, cryptography, and message exchange. The architectural layers are illustrated in Figure 4.1.

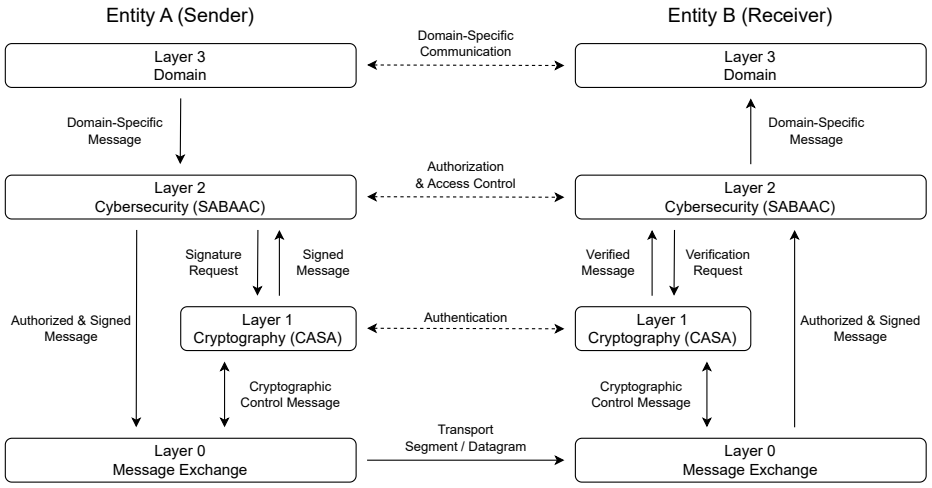

Figure 4.1.: Exemplary message exchange in four-layered CASC-SAS architecture.

4.1. Requirements & Adversarial Attacks

In the following, we introduce the requirements of the presented approach. Based on the identified requirements, functional and non-functional characteristics of the proposed approach are derived and evaluated. Each requirement is associated with a requirement category. The requirement categories consist of security, safety, availability, performance, and compatibility. With regard to information security, the approach has to satisfy seven requirements, namely device integrity, message integrity, authenticity, access control, non-repudiation, Principle of Least Privilege (PoLP), and Separation of Duties (SoD). In terms of safety, the approach must satisfy operational safety and fail-safe requirements. Furthermore, the approach must satisfy two availability-related requirements, namely operational continuity and fail-operational. With regard to performance, the approach has to take three constraints into account, namely communication latency, computational complexity, and energy as well as power. With regard to compatibility, the approach has to satisfy interoperability and interchangeability requirements.

In addition to the aforementioned requirements, the approach has to provide mitigation strategies against various types of attacks. The objective of these strategies is not merely to safeguard the equipment of the CASC-SAS approach, but rather to ensure the continuous operation of SAS devices, including intelligent electronic devices and merging units. The approach must be able to mitigate adaptive chosen-message, collusion, (distributed) denial-of-service, man-in-the-middle, replay, spoofing, and false data injection attacks. However, the approach does not address confidentiality-related requirements and attacks.

4.2. Certificateless Attribute-Based Server-Aided Authentication (CASA)

In the following section, we present the **C**ertificateless **A**ttribute-Based **S**erver-Aided **A**uthentication (CASA) concept. CASA is a CL-PKC approach. The goal of CASA is to provide cryptographic algorithms and schemes for key generation, key distribution, key revocation, signing, and verification. Moreover, the goal of CASA is to enable and support more abstract cybersecurity mechanisms like authorization and access control of the CASC-SAS approach. Therefore, CASA represents the foundation of the employed CASC-SAS cybersecurity mechanisms.

Since CASA is a CL-PKC approach, neither certificates nor key escrow is required [27]. Moreover, the CASA approach proposes a key generation that is not only based on subject identities but rather enables public keys and private keys based on arbitrary attributes of subjects or even groups of subjects. The key generation of the CASA approach is inspired by the alternative CL-PKC key generation technique proposed by Al-Riyami and Paterson [27]. The defining characteristics of the alternative key generation is the derivation of partial private keys from public keys and identities. As a consequence, an entity has to generate its public key before it can request a partial private key from the KGC. This alternative key

generation enables sending of partial private keys over unsecure channels and reduces the required trust in the KGC. Furthermore, this technique allows only one public key to be created for a specific private key.

4.2.1. Server-Aided Cryptography

As PKC mechanisms may consist of computationally complex algorithms and operations such as bilinear pairing, we propose a server-aided PKC approach. Therefor, we propose an extension of the CL-PKC concept and schemes to make time-critical steps server-aided. To make CASA server-aided, an Untrusted Cryptography Server (UCS) supports devices by handling computationally expensive algorithms instead of executing them locally on resource-constrained devices. To minimize the required trust, the UCS may only handle certain computations, i.e., partially sign or verify a request of a device. This server-aided approach enables resource-constrained devices to apply secure algorithms and schemes of CASA in a time-critical OT environment. In the following, we employ the concept of server-aided PKC for the verification process.

A server-aided verification process has to satisfy the property of being computation-saving [43]. A server-aided verification process V_{Aided} is computation-saving if the computational costs for the verifier are strictly less than the costs of non-server-aided verification $V_{Conventional}$. In other words, V_{Aided} is computation-saving if the equation $Cost(V_{Aided}) < Cost(V_{Conventional})$ holds.

4.2.2. Online & Offline Cryptography

Since CASA is tailored for time-critical communication, the approach aims to reduce the required time for cryptographic algorithms. In addition to server-aided cryptography, this time reduction is achieved by precomputation. For this purpose, each step of an algorithm is classified as either online or offline. Online steps depend on the sender's public key, the digital signature, or the message. Consequently, online steps cannot be precomputed. Nevertheless, specific online steps can be accelerated via server-aided cryptography. Offline steps depend on information that is available before any message exchange occurs. Therefore, offline steps can be precomputed to reduce the required time for cryptographic algorithms.

4.2.3. Signature Scheme $\mathcal{S}_{CASA}$

The CASA signature scheme $\mathcal{S}_{CASA} = (I, G_{VAL}, G_{PK}, G_{PPK}, G_{SK}, S, V_{ENT}, V_{SAV}, V_{FIN})$ is a nine-tuple of algorithms. The algorithms comprise an initialization algorithm I, a secret value generation algorithm G_{VAL}, a public key generation algorithm G_{PK}, a partial private key generation algorithm G_{PPK}, a private key generation algorithm G_{SK}, a signing algorithm S, a partial entity verification algorithm V_{ENT}, a partial server verification algorithm V_{SAV}, and a final entity verification algorithm V_{FIN}.

4.2.4. Security Model

The proposed signature scheme $\mathcal{S}_{CASA}$ is a secure signature scheme if it is existentially unforgeable under an adaptive chosen-message attack (EUF-CMA) [26, 44]. To create an existential forgery, i.e., output a valid pair of message and signature for a new message, an adversary carrying out a CMA can request valid signatures from an entity for any message of his choice. While non-adaptive CMA restricts the adversary to a fixed set of messages chosen prior to the attack, adaptive CMA allows the adversary to request signatures of messages depending on previously obtained signatures.

4.3. Server-Aided Attribute-Based Authorization & Access Control (SABAAC)

The second core concept of CASC-SAS is the **S**erver-Aided **A**ttribute-**B**ased **A**uthorization and **A**ccess **C**ontrol (SABAAC). The SABAAC approach enables the employment of attribute-based authorization and access control for time-critical SAS communication. Therefore, the approach prevents unauthorized access and extraction of information. The approach enables CASC-SAS to satisfy the access control, PoLP, and SoD security requirements. Moreover, the expressive and flexible but yet computationally expensive ABAC policies are handled in a server-aided manner to satisfy the strict time constraints of the SAS domain.

Our authorization and access control approach represents a cybersecurity concept that is located on the cybersecurity layer of the CASC-SAS architecture. Since the approach is located on the cybersecurity layer, it relies on secure authentication services provided by CASA. As a consequence, the approach assumes that efficient and secure signing and verification algorithms are available. In other words, CASA provides secure cryptographic algorithms and schemes that enable SABAAC to realize secure authorization and access control.

4.3.1. Authorization & Access Control Architecture

The proposed authorization and access control approach is based on a function-oriented component-based architecture. The architecture consists of four functional units. These functional units have been adapted from the access control mechanism functional points presented by Hu et al. [17]. Each functional unit is represented by a component that offers function-oriented services. The components of the architecture are TTPs since the semantic validity of their provided services is not verifiable by the service consumers. An overview of the SABAAC architecture, components, and protocols as well as the integration of CASA components and services into the SABAAC approach are shown in Figure 4.2.

Furthermore, SABAAC is divided into two central tasks or protocols. The first task is referred to as delegated attribute-based authorization. The delegated attribute-based authorization

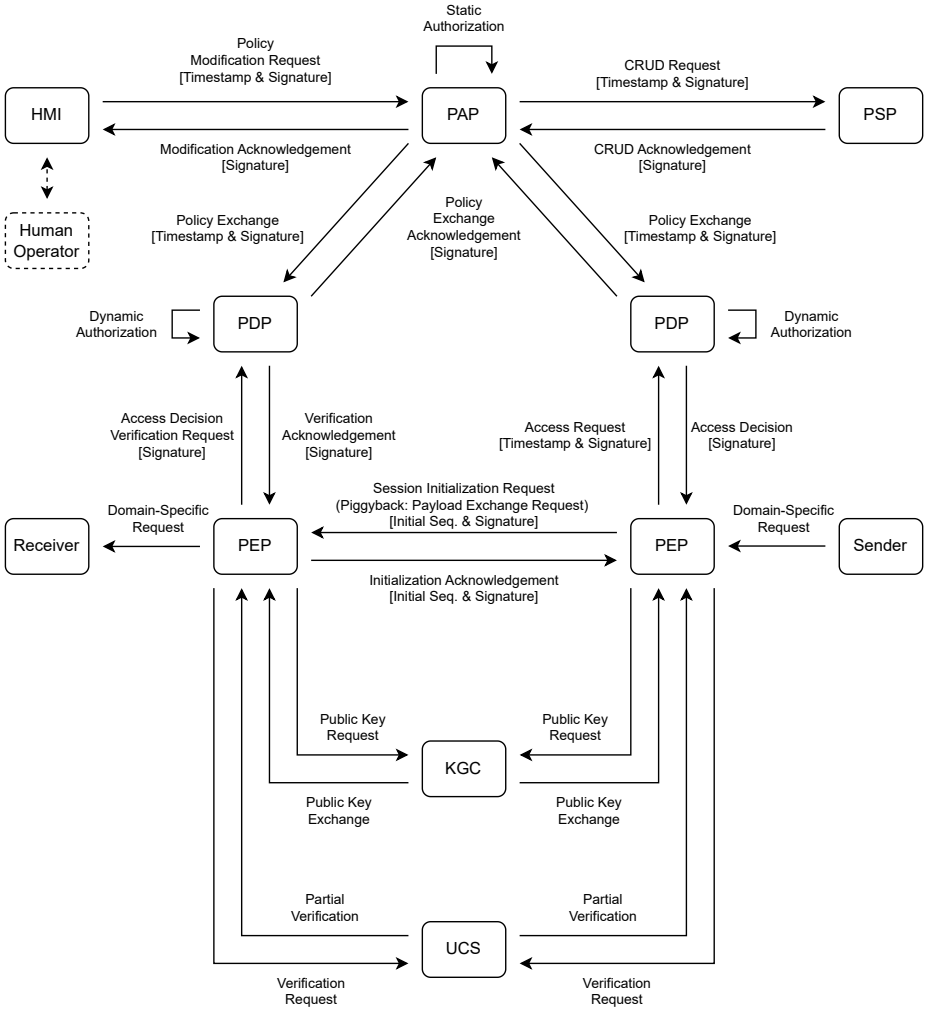

Figure 4.2.: Function-oriented component-based architecture of the SABAAC approach.

is responsible for the access control policy creation, management, storage, and distribution. This process partially takes place prior to occurring access requests and corresponding access decisions. The second central task is referred to as delegated ABAC. The delegated ABAC is responsible for the policy decision exchange and policy enforcement. This process takes place when an entity initiates the communication with another entity.

4.3.2. Access Control Policy

The SABAAC approach relies on the concept of attribute-based policies and access control due to the following benefits: ABAC enables multifactor policy expression, while RBAC and IBAC limit the policy expressiveness by only relying on either roles or identities. Consequently, the multifactor policy expression enables fine-grained and flexible access control. Moreover, the use of ABAC can avoid explicit authorizations prior to a request [17]. This dynamic evaluation allows the use of attributes from a time-variable environment. A

so-called real-time attribute represents an attribute whose value is time-dependent [37]. Given an attribute evaluation function E_{ATT} and a point of time t, the value λ_a of a real-time attribute a is defined by $E_{ATT}(a, t) = \lambda_a$. To handle policies based on their degree of time-variability, the SABAAC approach classifies policies as follows:

Dynamic Policy A dynamic policy ρ is an ABAC policy whose evaluation relies on at least one time-variable subject, object, environment, or action attribute. A policy ρ is dynamic iff $\exists a \in \rho : \exists t_i \neq t_j : E(a, t_i) \neq E(a, t_j)$. Due to the time-variable evaluation of dynamic policies, access decisions must have a limited time of validity that corresponds to the change rate of the underlying attribute values. As a result, caching of access decisions that are based on dynamic policies should be avoided. A dynamic policy is also referred to as real-time policy.

Static Policy A static policy ρ is an ABAC policy whose evaluation does not rely on time-variable subject, object, environment, or action attributes. A policy ρ is static iff $\forall a \in \rho : \forall t_i, t_j : E(a, t_i) = E(a, t_j)$. Since static policies do not rely on time-variable attributes, access decisions can be cached. Moreover, due to the non-frequent attribute retrieval and evaluation as well as access decision caching, static policies are a viable solution for low latency message exchange. A static policy is also referred to as non-real-time policy.

4.4. Realization

In the following section, we discuss the proposed realization of the CASC-SAS approach and its two core concepts CASA and SABAAC. The approach and its two concepts introduce components that are defined and discussed in section 4.2 and section 4.3. These components have to be integrated into the SAS architecture to employ the CASC-SAS approach. This integration of CASC-SAS components into the SAS architecture is visualized in Figure 4.3. The components depicted in blue represent elements of the SAS architecture, whereas the components depicted in red are introduced by the CASC-SAS approach. The components with a color gradient represent elements of the SAS architecture that have been adapted to support CASC-SAS concepts. The PEP, PDP, UCS, and KGC components have to be present locally in every adapted SAS. This is necessary due to the strict time constraints of SAS-internal low latency message exchange. The PAP and PSP instances may be centrally deployed, since static authorization is part of the non-time-critical control path communication. Any non-intermediate SAS component that participates in a communication relationship must either support the CASC-SAS protocols or use the services provided by a PEP to secure occurring message exchanges.

To examine the feasibility and perform the above-mentioned integration, we propose a hardware and software realization of our approach. The aim of the realization is to provide implementations of CASA and SABAAC with a full range of functions. The software is going to be implemented component-wise using high-level programming languages. Depending on the complexity and time constraints of a specific component, different programming

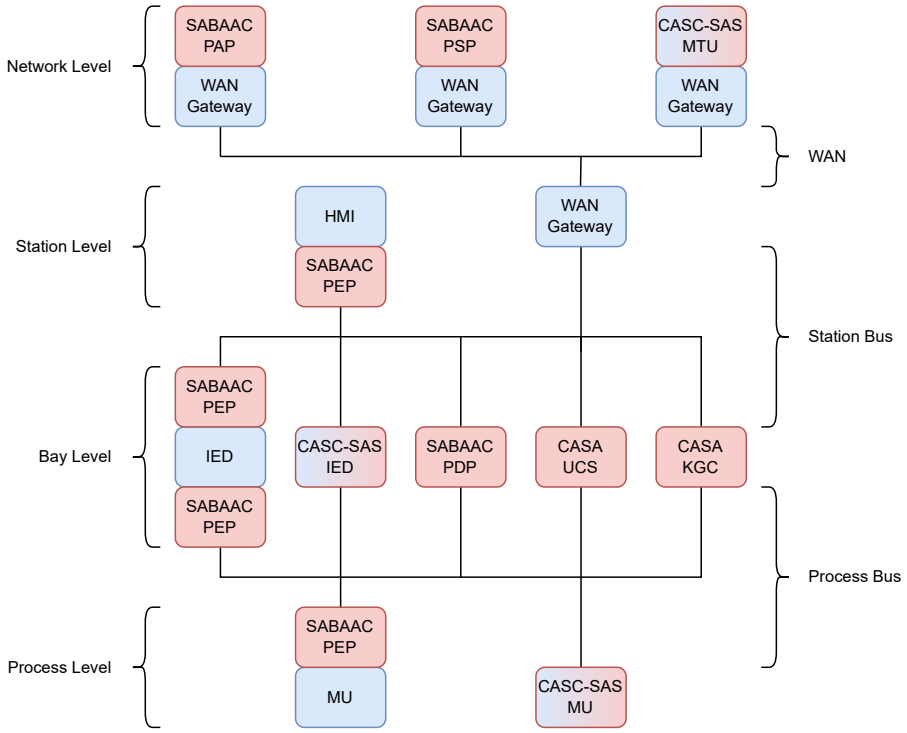

Figure 4.3.: Adaptation of the layered SAS architecture to the CASC-SAS approach.

languages might be used for the implementation. Due to internal dependencies, the software implementation is split into two parts. The first part is dedicated to the CASA approach, as it represents the foundation of all employed protocols. The second part is dedicated to the SABAAC components and protocols.

The employed components of CASA and SABAAC provide different services. Furthermore, the components have to be deployed differently to correspond to the proposed protocols. While PAP and PSP may be deployed centrally, components such as PEP, PDP, UCS, and KGC are distributed to individual SAS instances. This leads to differing hardware requirements for the implemented components. Moreover, except for PEP instances, the components provide their services by using a client-server pattern. The PEP instances partially use a client-server pattern and partially provide their services in the form of a Bump-In-The-Wire (BITW) solution. The services provided by PEP instances via BITW pattern are automatically applied to captured packets. Therefore, these services are invisible to the corresponding service consumers. This BITW pattern is inspired by the security filter approach presented by Ishchenko and Nuqui [14]. Taking the differing provision patterns and deployment structures into account, we propose the usage of performance-oriented server hardware for the PAP, PSP, PDP, UCS, and KGC to avoid bottlenecks and mitigate the risk of accidental or malicious DoS. Moreover, we propose the usage of inexpensive off-the-shelf hardware for the highly distributed PEP instances.

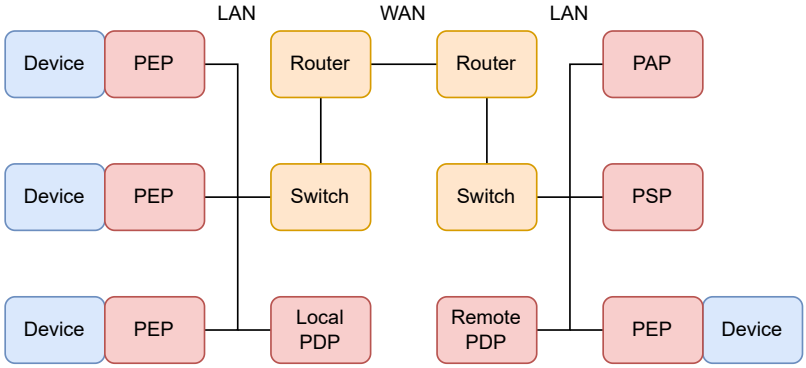

Figure 4.4.: Architecture of the network test bed.

4.5. Evaluation

In this section, the evaluation of the CASC-SAS approach is discussed. The goal of the evaluation is to derive quantitative and qualitative metrics of the approach for different areas of interest. These metrics are used to verify the applicability and to identify limitations of the proposed approach. We propose three areas of interest for the evaluation of the CASC-SAS approach:

Security Evaluation Does CASC-SAS provide security against typical SAS adversaries and attacks? Which security, safety, and availability requirements are satisfied? Which system and adversary characteristics were assumed? Did the attack surface change?

Performance Evaluation Is CASC-SAS capable of securing time-constrained communication of an SAS? Which performance requirements are satisfied? Which communication characteristics were assumed? Which types of messages are supported? Is the approach resistant against network exceptions including congestion, delay, jitter, duplicated packets, lost packets, and out-of-order packet delivery?

Compatibility Evaluation Is CASC-SAS a feasible solution for the construction or retrofitting of an SAS? Which compatibility requirements are satisfied? Which device characteristics were assumed? How high are the additional costs for SAS construction and retrofitting?

The evaluation is performed theoretically as well as experimentally. For the theoretical parts of the evaluation, formal and informal methods are used to proof certain characteristics of the proposed approach. The experimentally performed part of the evaluation is based on the realization presented in section 4.4. Based on the realization, a network simulation and network test bed, visualized in Figure 4.4, are constructed. The simulation strategy has the advantage of repeatability and reproducibility due to deterministic behavior, whereas the behavior of the test bed is non-deterministic. The test bed results are practice-oriented and transferable to the physical SAS domain, whereas the behavior of a real SAS cannot be compared to the deterministic behavior of the network simulation.

5. Project Plan

In the following section, the project plan of the proposed master's thesis is discussed. The project plan consists of a work plan and risk assessment. The work plan defines the project objectives, milestones, tasks, and deliverables and is presented in section 5.1. The time schedule represents the mapping of the proposed work plan to Calendar Weeks (CW) and is visualized in Figure 5.1. The risk assessment evaluates technical and non-technical risks for the proposed project plan and is discussed in section 5.2.

5.1. Work Plan

The work plan structures the proposed thesis into six milestones. Each milestone represents a major phase of the proposed master's thesis. The milestones serve as intermediate project goals which enable monitoring and reporting of project progress. Each milestone is defined by its duration in CWs, deliverables, and tasks. Each milestone consists of at least one task. A task of a milestone is referred to as increment. The duration of a milestone depends on the duration of its increments and increment interdependencies. Multiple increments mapped to the same calendar weeks may be performed in parallel, as there are either no interdependencies or existing dependencies can be resolved beforehand. The projected timescales for the completion of milestones and increments are calculated based on empirical values. The milestones of the proposed master's thesis are defined as follows:

Milestone I: Preliminary Work

Duration: 14 Weeks (15. April 2024 (CW 16) – 22. July 2024 (CW 30))

Deliverables: Master's thesis proposal

Milestone II: Realization

Duration: 11 Weeks (22. July 2024 (CW 30) – 07. October 2024 (CW 41))

Deliverables:
a) Software Design, Implementation, Tests (Unit, Integration, and System), & Test Coverage Report of CASC-SAS
b) Hardware Deployment Scripts of CASC-SAS
c) Thesis Chapter: Realization

Increments:
1) Design, Implementation, Tests, & Deployment of SABAAC (7 Weeks)
2) Design, Implementation, Tests, & Deployment of CASA (7 Weeks)

3) Architecture & Code Review (Optional, Single Meeting)
4) Writing of Documentation (2 Weeks)

Milestone III: Evaluation

Duration: 7 Weeks (07. October 2024 (CW 41) – 25. November 2024 (CW 48))

Deliverables: a) Evaluation Results of CASC-SAS
b) Thesis Chapter: Evaluation

Increments: 1) Security Evaluation (3 Weeks)
2) Performance Evaluation (3 Weeks)
3) Compatibility Evaluation (1 Weeks)
4) Writing of Documentation (2 Weeks)

Milestone IV: Conclusion

Duration: 2 Weeks (25. November 2024 (CW 48) – 09. December 2024 (CW 50))

Deliverables: a) Thesis Chapter: Conclusion
b) Thesis Chapter: Limitations
c) Thesis Chapter: Future Work
d) Thesis Chapter: Abstract

Increment: Writing of Documentation: Conduct a review of results and derive a conclusion, limitations, and future work with regard to the research questions (2 Weeks)

Milestone V: Review

Duration: 5 Weeks (09. December 2024 (CW 50) – 13. January 2025 (CW 03))

Deliverables: Reviewed & Proofread Master's Thesis

Increments: 1) Internal Review: Proofreading & Correction by the Authors (2 Weeks)
2) External Review: Proofreading & Correction by External Readers (4 Weeks)

Milestone VI: Finalization

Duration: 6 Weeks (09. December 2024 (CW 50) – 20. January 2025 (CW 04))

Deliverables: a) Printed & Bound Master's Thesis
b) Master's Thesis Presentation Slides

Increments: 1) Thesis Presentation Preparation (5 Weeks)
2) Printing & Binding of Thesis (1 Week)

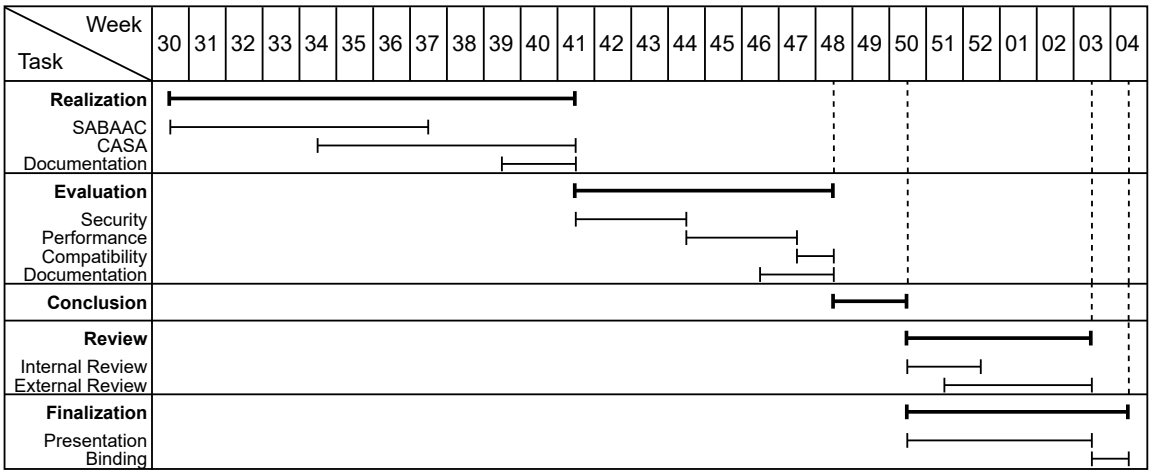

Figure 5.1.: Time schedule of the proposed master's thesis.

5.2. Risk Assessment

The risk assessment identifies potential risks and assesses their impact on the proposed project plan. Additionally, it presents mitigation strategies for the identified risks. By considering the occurrence of undesirable events, the risk assessment enables the meeting of deadlines. The identified and assessed risks are classified as either technical or non-technical risks. The technical risks are discussed in detail in subsection 5.2.1. The non-technical risks consist of organizational and project management risks and are discussed in detail in subsection 5.2.2.

5.2.1. Technical Risks

The following technical risks represent deficiencies in the design and implementation of the approach, which could result in non-compliance with stated requirements. To ensure the compliance with stated requirements, it is recommended that software testing and system evaluation are conducted in an automated manner.

Software Design Flaws Software design flaws have an impact on the performance, availability, security, and safety of the approach. To mitigate the risk of software design flaws and therefore avoid re-implementation, architecture reviews are conducted after the design of the CASC-SAS software. Furthermore, automated acceptance tests check the compliance of already implemented software with stated system requirements to identify software design flaws.

Software Implementation Flaws Software implementation flaws have an impact on the performance, availability, security, and safety of the approach. Implementation flaws such as bugs are avoided by using automated software testing. The automated software testing consists of unit, integration, system, and acceptance tests. The unit, integration, and system tests assure the correct and failure-free operation of the software under

valid and invalid system conditions. The acceptance tests check the compliance with stated system requirements. The employed software testing methods have to provide high source code coverage. Besides automated software testing, code reviews after the implementation of the CASC-SAS software can increase the source code quality and mitigate the risk of implementation flaws.

Transient Hardware Faults Transient faults of system hardware have an impact on the performance and availability of the approach. Transient faults have to be taken into account during the design and implementation of the system. This can be achieved by employing failure-avoidance strategies such as redundancy and automated system monitoring.

Persistent Hardware Faults Persistent faults of system hardware have an impact on the performance and availability of the approach. Persistent faults have to identified via automated system monitoring and resolved by replacing corresponding hardware components.

Unsuitable Hardware Unsuitable hardware has an impact on the performance and economic aspects of the approach. As a consequence, unsuitable hardware has to be replaced by suitable hardware to satisfy the system requirements. To make the approach performant and economically feasible, the system has to use components that provide neither too much nor too less performance for their designated tasks.

5.2.2. Organizational & Project Management Risks

The following risks represent deficiencies in the project organization and management. To mitigate the following risks, a preliminary milestone was created with the objective of reducing the number and complexity of tasks to be completed within the limited thesis period.

Inaccurate Estimation of Milestone & Increment Duration The projected durations of milestones and increments are calculated based on empirical values. However, this calculation approach may result in inaccurate estimations, which could lead to a deviation from the proposed time schedule. To mitigate the risk of inaccurate estimations, an additional buffer time is included in each duration associated with an increment or milestone.

Illness-Related Delay Illness may result in a deviation from the proposed time schedule. Small deviations, in the order of weeks, can be compensated by the additional buffer times. Large deviations, in the order of months, require either an extension of the limited thesis period or a prioritization of increments. The possibility of extending the thesis period by up to three months is governed by the examination regulations.

Bibliography

[1] Keith Stouffer et al. *Guide to Operational Technology (OT) Security*. Tech. rep. NIST Special Publication 800-82,Rev.3. National Institute of Standards and Technology, 2023. DOI: 10.6028/nist.sp.800-82r3.

[2] Evelio Padilla. *Substation Automation Systems: Design and Implementation*. Wiley, Oct. 2015. ISBN: 9781118987216. DOI: 10.1002/9781118987216.

[3] Occupational Safety and Health Administration (OSHA). *Illustrated Glossary - Substations*. URL: https://www.osha.gov/etools/electric-power/illustrated-glossary/sub-station (visited on 08/02/2024).

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

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

[6] 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).

[7] Communications Security Establishment Canada. *Cyber threat bulletin: Cyber threat to operational technology*. Dec. 2021. URL: https://open.canada.ca/data/dataset/98bad300-28f1-49b9-9b34-2d46de4c9a58 (visited on 08/03/2024).

[8] Jonathan Fildes. *Stuxnet worm targeted high-value Iranian assets*. 2010. URL: https://www.bbc.com/news/technology-11388018 (visited on 08/03/2024).

[9] Jim Finkle. *Exclusive: Insiders suspected in Saudi cyber attack*. 2012. URL: https://www.reuters.com/article/net-us-saudi-aramco-hack/exclusive-insiders-suspected-in-saudi-cyber-attack-idUSBRE8860CR20120907 (visited on 08/03/2024).

[10] Cybersecurity & Infrastructure Security Agency (CISA). *Cyber-Attack Against Ukrainian Critical Infrastructure*. 2021. URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (visited on 08/03/2024).

[11] Natalia Zinets. *Ukraine hit by 6,500 hack attacks, sees Russian cyberwar*. 2016. URL: https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC (visited on 08/03/2024).

[12] Cybersecurity & Infrastructure Security Agency (CISA). *CrashOverride Malware*. 2021. URL: https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware (visited on 08/03/2024).

[13] Blake Johnson et al. *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*. 2017. URL: https://cloud.google.com/blog/topics/threat-intelligence/attackers-deploy-new-ics-attack-framework-triton (visited on 08/03/2024).

[14] 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.

[15] 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.

[16] National Institute of Standards and Technology. "Personal Identity Verification (PIV) of Federal Employees and Contractors". In: *Federal Information Processing Standards Publication (FIPS PUB)* 201-3 (2022).

[17] 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.

[18] 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.

[19] Elaine Barker and William Barker. *Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*. Tech. rep. NIST Special Publication 800-175A. National Institute of Standards and Technology, 2016. DOI: 10.6028/NIST.SP.800-175A.

[20] Elaine Barker. *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. Tech. rep. NIST Special Publication 800-175B,Rev.1. National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-175Br1.

[21] CNSS Glossary Working Group. "CNSS Glossary". In: *Committee on National Security Systems Instruction (CNSSI)* 4009 (2022).

[22] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. DOI: 10.1201/9780429466335.

[23] Claudia Eckert. *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. De Gruyter, Jan. 2023. ISBN: 9783110985115. DOI: 10.1515/9783110985115.

[24] Auguste Kerckhoffs. "La cryptographie militaire". In: *Journal des sciences militaires* IX (1883).

[25] C. E. Shannon. "Communication Theory of Secrecy Systems". In: *Bell System Technical Journal* 28.4 (Oct. 1949), pp. 656–715. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[26] Dan Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography*. 2023. URL: https://toc.cryptobook.us/book.pdf (visited on 06/22/2024).

[27] Sattam S. Al-Riyami and Kenneth G. Paterson. "Certificateless Public Key Cryptography". In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2003, pp. 452–473. ISBN: 9783540400615. DOI: 10.1007/978-3-540-40061-5_29.

[28] Amit Sahai and Brent Waters. "Fuzzy Identity-Based Encryption". In: *Advances in Cryptology – EUROCRYPT 2005*. Springer Berlin Heidelberg, 2005, pp. 457–473. ISBN: 9783540320555. DOI: 10.1007/11426639_27.

[29] Vipul Goyal et al. "Attribute-based encryption for fine-grained access control of encrypted data". In: *Proceedings of the 13th ACM conference on Computer and communications security*. CCS06. ACM, Oct. 2006. DOI: 10.1145/1180405.1180418.

[30] Vincent C Hu. *Overview and considerations of access control based on attribute encryption*. Tech. rep. NIST Internal Report 8450-upd1. National Institute of Standards and Technology (U.S.), 2023. DOI: 10.6028/nist.ir.8450-upd1.

[31] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-Policy Attribute-Based Encryption". In: *2007 IEEE Symposium on Security and Privacy (SP '07)*. IEEE, May 2007. DOI: 10.1109/sp.2007.11.

[32] Jin Li et al. "Attribute-based signature and its applications". In: *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. ASIA CCS '10. ACM, Apr. 2010. DOI: 10.1145/1755688.1755697.

[33] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. "Attribute-Based Signatures". In: *Topics in Cryptology – CT-RSA 2011*. Springer Berlin Heidelberg, 2011, pp. 376–392. ISBN: 9783642190742. DOI: 10.1007/978-3-642-19074-2_24.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] Mingchao Ma and Steve Woodhead. "Authentication delegation for subscription-based remote network services". In: *Computers & Security* 25.5 (July 2006), pp. 371–378. ISSN: 0167-4048. DOI: 10.1016/j.cose.2006.03.006.

[41] 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.

[42] H. Samuel, W. Zhuang, and B. Preiss. "Routing over Interconnected Heterogeneous Wireless Networks with Intermittent Connections". In: *2008 IEEE International Conference on Communications*. IEEE, 2008. DOI: 10.1109/icc.2008.435.

[43] Wei Wu et al. "Server-Aided Verification Signatures: Definitions and New Constructions". In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2008, pp. 141–155. ISBN: 9783540887331. DOI: 10.1007/978-3-540-88733-1_10.

[44] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks". In: *SIAM Journal on Computing* 17.2 (Apr. 1988), pp. 281–308. ISSN: 1095-7111. DOI: 10.1137/0217017.

A. Appendix

A.1. Review Questions & Responses

Q1. *Unclear context of OT-related cybersecurity incidents (p. 2)* — The context of the cybersecurity incidents was clarified by rephrasing the sentence and moving the citation to a more appropriate position.

Q2. *Textual citation of 3 or more authors should be shortened to et al. (p. 2 ff.)* — The maximum number of author names in textual citations was limited to two, e.g., (Elbez, Keller, and Hagenmeyer [16]) becomes (Elbez et al. [16]).

Q3. *Typo in the word therefore (p. 2)* — A missing letter was added to the word therefore.

Q4. *Research questions should relate to previously described challenges, and RQ1 and RQ2 should differ more from each other (p. 2)* — All three research questions were partially reconstructed to relate to the security objectives. Moreover, the research questions were rephrased to clarify their goals.

Q5. *Interchanged words in contribution section (p. 3)* — The corresponding sentence was rephrased.

Q6. *To which extent is the SABAAC approach flexible (p. 3)* — Since its policies and not the approach is expressive and flexible, the sentence was rephrased. Moreover, the expressiveness, flexibility, and computationally expensiveness of the policies were further clarified.

Q7. *It would be good to relate the fundamentals to the field of application (p. 6)* — Since the fundamentals were shortened from twenty to two pages, the relations between its topics and the OT/ICS/SAS-domain were lost. Moreover, the relevance of the more abstract topics including access control and cryptography for the OT-domain is not sufficiently described in the proposal. This will be added to the fundamentals chapter of the thesis, as the realization is currently an open question.

Q8. *A paragraph could be added to relate the related work chapter to the fundamentals (p. 7)* — This relation is present in the long thesis proposal in the form of a division into sections, which are related to topics of the fundamentals.

Q9. *Please consider organizing the related work into sections (p. 7)* — This organization is present in the long thesis proposal and will be transferred to the final master's thesis. Moreover, an extension for the cryptography-specific related work is planned.

Q10. *Please consider discussing some limitations of related works on ABAC and RBAC to justify the motivation of your work (p. 8)* — The similarities and differences of the thesis and related work as well as the limitations of related work are present in the long thesis proposal.

Q11. *Cybersecurity and cryptography are names of CASC-SAS layers (p. 9)* — The differences of the two layers are discussed in detail in the long thesis proposal. However, since the two words cybersecurity and cryptography are closely related, renaming or renumbering of the layers is currently under consideration.

Q12. *For ease of read, better present requirements as a list (p. 10)* — In the long thesis proposal the requirements and their short descriptions are presented as a list.

Q13. *How does the integration of CASA effectively relate to figure 4.2 (p. 13)* — This figure caption was shortened, and the CASA-specific part was removed for better understandability.

Q14. *Which adversarial attacks would be relevant as use cases (p. 16)* — A subsection in the system model dedicated to relevant attacks and attack trees is planned for the final thesis. Moreover, relevant attacks were added to the short proposal's requirements section. Due to the limited space in the short proposal, no attack-specific section with enumerated attacks was added.

Q15. *Which considerations would be included in the economic evaluation (p. 16)* — Besides the aspects mentioned in the proposal, metrics such as the cost of CASC-SAS equipment will be discussed in the economic evaluation. Moreover, the economic evaluation covers the compatibility-related requirements, including interoperability and interchangeability, which are core concepts of the IEC 61850.

Q16. *Which evaluation aspects are possible theoretically (p. 16)* — The theoretical evaluation covers the security proofs of CASA, the economic evaluation, and the calculation of minimum transfer time requirements for the performance evaluation. The theoretical approaches used will be discussed in detail in the corresponding evaluation sections in the thesis.

Q17. *Are times in the work plan total times and are increments processed in parallel (p. 17)* — To clarify the total durations of milestones and parallel execution of increments, a sentence was added to the work plan introduction.

Q18. *Shouldn't software design flaws be considered before software implementation flaws (p. 20)* — The order of the risks was changed to clarify that the design should be flawless before the implementation.

Q19. *The figure captions are too long* — All figure captions in the proposal were shortened.

Q20. *The fundamentals are lacking a cryptography section* — A cryptography section covering symmetric and asymmetric cryptography was added to the fundamentals of the long proposal.

Q21. *The NIST recommendations for access control are not discussed in the fundamentals* — A NIST recommendations section was added to the fundamentals of the long proposal.

Q22. *The security model of CASA makes very strong statements about EUF-CMA, which are not correct anymore* — The strong statement was removed from the security model and the section was rephrased.

Q23. *The introduction chapter lacks an objective section* — A section for the objective of the thesis was added to the introduction chapter. Moreover, the already existing research question section was integrated into the new section.

Q24. *The introduction chapter lacks a thesis structure section* — A section for the proposed structure of the thesis was added to the introduction chapter of the long proposal. Moreover, a graphical representation of the structure is currently under consideration.

Q25. *The typical cybersecurity incidents mentioned in related work are not present in the objective of the approach* — A paragraph for cybersecurity incidents was added to the objective section.

Q26. *Sender and receiver are interchanged in SABAAC figures* — The errors in the SABAAC figures were fixed.

Q27. *SABAAC is misspelled in the time schedule* — The error in the time schedule figure was fixed.

Q28. *A deprecated security requirement is present in the CASA description in the long proposal* — The deprecated security requirement was removed.

Q29. *Prof. Dr. Veit Hagenmeyer is the first examiner of the thesis* — The examiners on the title page of the short and long proposal were changed. However, the second examiner is currently unknown.

Q30. *Missing group logo at title page* — The KASTEL logo was added to the title page as group logo.

Q31. *Citations should be numbered in the order in which they appear* — The ordering of the bibliography was changed.

Q32. *State-sponsored cybersecurity incidents included summary of incidents from 2013 to 2020 (p. 2)* — The mentioning of non-discussed but referenced incidents from 2013 to 2020 was removed.

Q33. *Ordering of research questions is not consistent with main thesis focus ABAC (p. 2)* — Changed order of RQ1 and RQ2.

Q34. *RQ2 and RQ3 contain concepts of contribution and shrink the solution space too much (p. 2)* — Revised research questions by replacing concrete concepts such as certificateless and server-aided with more goal-oriented and unbiased terms such as lightweight and scalable.

Q35. *Introduction chapter lacks an enumeration of thesis contributions (p. 3)* — The contribution section was rephrased and restructured. The contributions are now presented as an enumeration.

Q36. *The asymmetric cryptography section should be renamed to PKC and lacks a description of symmetric cryptography (p. 5)* — The PKC section was renamed and a sentence to distinguish symmetric from asymmetric algorithms was added. The long version of the proposal contains an own section for symmetric cryptography.

Q37. *The economic evaluation is not possible due to missing data and the term economic/economy should be avoided (p. 16)* — The third evaluation area was renamed to compatibility, to emphasize the new focus on interoperability and interchangeability as defined in IEC 61850, and the focus on economy in this area was reduced by rephrasing and restructuring.

Q38. *Overlapping increments of time schedule do not seem feasible (p. 19)* — The realization phase was extended, and the evaluation phase was shortened by two weeks. Moreover, the increment durations and starting dates were revised to reduce overlapping phases.