Human Systems Engineering and Design (IHSED 2024), Vol. 158, 2024, 289–297
https://doi.org/10.54941/ahfe1005552

From System High to Zero Trust: The Impact of Security Requirements on a Multinational Standard With Technical Specifications for Data Dissemination

Lorraine Hagemann and Philipp Klotz

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB,
Fraunhoferstr. 1, 76131 Karlsruhe, Germany

ABSTRACT

Technical and technological progress leads to new possibilities for information exchange systems. Particularly, the associated aspects of IT security are continuously evolving. In addition, information is nowadays most of the time stored decentralized and not close to the user working with it. Information is disseminated over different network nodes and geolocations. This leads to the necessity of integrating heterogeneous external and internal systems and applications. As a result of these conditions, new requirements as well as risks to the underlying systems are being identified. Technological progress also opens up new opportunities for attackers and provides additional targets. This is extremely challenging for systems that support data exchange based on a multinational standard such as Coalition Shared Data (CSD). CSD is a concept for the distribution of information in multinational Joint ISR (Intelligence, Surveillance and Reconnaissance) operations. The interfaces, data models and specifications to support this concept are described in the STANAG (STANdardization AGreement) 4559. In order to fulfill the security requirements of a current multinational environment, zero trust architecture is now enforced. In this paper we investigate the compatibility of the zero trust architecture with the current version of STANAG 4559 Edition 4. Here we focus on a specific part of the standard that deals with the storage and dissemination of Joint ISR products. We point out working fields in the areas of authentication, authorization, data integrity and legacy technologies. As the latter is a core problem, our main focus in this paper is the replacement of legacy technology through the communication architecture REST (Representational State Transfer). We highlight the challenges associated with such changes. We explain how the STANAG 4559 Custodian Support Team (CST) deals with these challenges. We also describe how we support these aspects by providing definitions, prototyping and participating in the test events with our implementation.

Keywords: STANAG, Coalition shared data, Zero trust, System high, Interoperability

INTRODUCTION

Information exchange systems are indispensable nowadays. Information should be available at any time and from anywhere to those who are interested in that specific data. Together with new requirements, technical and technological progress must also be considered. The corresponding trends and best practices are subject to constant changes especially in case of IT security requirements. Progress has opened up new opportunities for attackers and the techniques used by attackers have evolved. This is extremely challenging for systems that support data exchange based on a multinational standard such as Coalition Shared Data (CSD).

CSD is a concept for the information distribution in multinational Joint ISR (Intelligence, Surveillance and Reconnaissance) operations. The interfaces, data models and specifications to support this concept are described in a NATO standard called STANAG (STANdardization AGreement) 4559 (NATO Standardization Office (NSO), 2018a). In a military environment, getting information to the right person at the right time is critical. This enables decision-makers to react in an appropriate manner to situations as they arise. Especially when several nations are involved and acting as a coalition, data exchange is essential.

Developments in recent years have given rise to new risks that have not (yet) been considered to the same extent in previous security concepts. In order to fulfill the security requirements of a multinational environment, which have become more stringent in recent years, a shift to a zero trust architecture (ZTA) is now required. The term “zero trust” describes a design paradigm that is based on the principle of minimal privileges for all users, devices and systems. This means that, in contrast to a system high architecture, there is no implicit trust between all involved entities, requiring dedicated security measures for all levels. For the migration of the standard from a system high architecture to a ZTA we analyzed the underlying systems and processes and identified three main working fields: legacy technology, access control and data integrity. These working fields and the resulting adjustments to the standard will be subject of this paper.

The paper is structured as follows: In the chapter *ZERO TRUST* we introduce the concept of ZT and the corresponding requirements. In order to adapt a ZTA to the STANAG 4559, we look at the resulting working fields and the necessary adjustments for the standard in the chapter *STANAG 4559 AND ZERO TRUST.* The implementation of these adjustments in our system is presented in chapter *ADAPTIONS IN OUR SYSTEM AND TESTING*. Finally, the paper concludes with a summary and possible next steps.

ZERO TRUST

As a consequence of the digital age, the amount of services, devices and systems, even from external sources, had a rapid growth and the environment has become more complex over the years. Because of that, perimeter-based network security is not sufficient anymore. On the one hand it is difficult to identify a single perimeter for the whole enterprise, on the other hand the perimeter becomes a single source of failure. If attackers manage to overcome the perimeter, the enterprise is not secured at all. Therefore, the entities are not trusted implicitly, regardless of their physical or network location. To overcome the mentioned security concerns, the concept ZT and the ZTA was defined in the NIST Special Publication 800–207 "Zero trust Architecture" (Stafford, 2020) as follows:

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

The concept of ZT represents a paradigm shift in the field of cyber security. Rather than addressing the vulnerabilities associated with users, this approach also encompasses the security of assets with the main focus on resources. Nonetheless, actually all enterprise assets and subjects should be protected, e.g. devices, components, applications and user. To reduce the risk of attackers, including attacks from the inside of the network, the access to resources should be minimized by limiting access according to the need-to-know principle. This principle is based on the premise that only users who require access to resources in order to fulfill their task, are granted such access. This includes continuous authentication and authorization of the identity and security status of the resource with every access request. The enforcement of a fine granular access control is the key of a ZTA. In order to achieve this, the NIST (Stafford, 2020) has defined seven basic tenets:

1. Every data source and computer service of the enterprise environment is considered as a resource.
2. The communication-security is location independent. This implies that there is no implicit trust based solely on the network location of the resource. In particular, access requests originating from within the environment must comply with the same rigorous security requirements as those originating from outside.
3. The access to a resource is evaluated and granted session-based.
4. Access is accomplished through the evaluation of policies and access rules.
5. Assets are not automatically considered trustworthy. To assess the trustworthiness of an asset, the integrity and security posture of each asset must be monitored.
6. Resource authentication and authorization is dynamically and validated before granting access.
7. The state of assets, network infrastructure and communication is monitored and collected. Furthermore, the collected information is logged and should be used to improve the system regarding security aspects.

To implement ZT fully, the environment must guarantee the seven basic tenets. In cases where it is not a new implementation, existing systems and services must be migrated. Such a migration is challenging to realize within a single iteration of implementation. It is therefore necessary to conduct this migration step by step.

STANAG 4559 AND ZERO TRUST

In this chapter we will discuss the potential for a multinational standard for data dissemination to support a ZTA.

In particular we will consider the STANAG 4559 standard. The standard is used for the exchange of military Joint ISR data on multiple levels. This includes IRM&CM (Intelligence Requirements Management & Collection Management) data as well as live data from sensor systems as well as Joint ISR products as images, documents, report (Essendorfer et al., 2018). It describes an overall concept that makes it possible to connect different systems from different vendors in a network. Consequently, the standard defines common interfaces, use cases and processes to permit the fundamental dissemination of data. The current version of the standard, Edition 4, is divided into three documents. These documents describe the three principal parts and data types provided by the standard: AEDP (Allied Engineering Documentation Publications)-17 (NATO Standardization Office (NSO), 2018b) (static data), AEDP-18 (NATO Standardization Office (NSO), 2018c) (dynamic data) and AEDP-19 (NATO Standardization Office (NSO), 2018d) (streaming data). To (further) develop the standard and its AEDPs, the STANAG 4559 Custodian Support Team (CST) was established. As a member of this multinational team we contribute to the adaption for the standard.

In the following sections, our analyses and observations will focus exclusively on AEDP-17. A system that implements the AEDP-17 is called a CSD-Server. Besides the standardized interfaces for ingesting and retrieving data, a synchronization concept is designed to disseminate data between different implementations (by different vendors/ nations) in the standard. As we outlined in earlier work, "*to reduce network bandwidth, only the catalogue entry is synchronized automatically. The product itself (image, video, etc.) is normally only shared if requested by a (client) system.*" (Kerth et al., 2019).

The available metadata of the catalog entry is defined by a standardized data model. This enables the underlying ISR product to be described by using optional and mandatory attributes. This means that e.g. an image can be catalogued (and thus be queried) among other attributes by its creator, the date/time it was created, the geocoordinates it covers, the format it is stored in and the security attributes it has. Additionally, extensions can be defined and integrated to expand the basic data model (e.g. to cover more data types or different attributes). This offers the opportunity to introduce new functionalities in the existing standard. Suitable extensions can also be adopted as fixed components for future versions of the standard.

The origins of the STANAG 4559 lie in the early 2000s. At that time, assuming networks and systems could provide ultimate security, a system high approach with implicit trust seemed to be sufficient. Therefore, the adoption of the system high architecture for the standard was agreed upon. The term system high refers to a security configuration that has been implemented to protect sensitive or classified information within a system from external attackers. All users that have access to the system must be in possess of a valid clearance for all information available in the system (Computer Security Center (US), 1985). Developments in recent years have given rise to new risks that have not (yet) been considered in the STANAG sufficiently. In order to fulfill the security requirements of a multinational environment, which have become more stringent in recent years, a shift to a ZTA is now demanded.

As outlined in the NIST, the migration to ZT is an iterative process. In the first step, we therefore analyzed possible consequences for the standard resulting from a migration to ZT. The standard is based on implicit trust which already contradicts tenet number 2 of ZT. In order to replace implicit trust, we have identified initial working fields, which we present in the following subsections.

Legacy Technology

The very first recommended step for migration is the analysis of the existing processes (Stafford, 2020). Our analysis showed that the use of the legacy technology CORBA (Common Object Request Broker Architecture) itself is a challenge for the migration ZT. As described in (Henning, 2006), CORBA is and was a complex technology. Especially the complex API and the non-transparent IOR (Interoperable Object References) were criticized. As a result of its complexity and the introduction of alternative technologies, CORBA became outdated, e.g. CORBA is no longer supported in the LTS version of JAVA since JAVA SE11 (Andersen, 2017). This makes it difficult to find technical experts who are still involved with CORBA. Comprehensive changes and further developments of the standard are therefore difficult and time-consuming.

Additionally, according to (Henning, 2006) the use of CORBA has flaws considering security aspects: CORBA was mainly used inside a company's network and the communication was protected by a firewall from external networks. For this a port must be opened in the corporate firewall, which conflicts often with security policies. Furthermore, traffic is encrypted, which allows eavesdropping and man-in-the-middle attacks.

Due to the flaws of CORBA the CST has decided to replace CORBA. Since CORBA is firmly established in the standard this is no trivial process. A potential solution must guarantee backward compatibility such that CSD-Server of deviating versions of the standard are still able to communicate with each other.

As a replacing technology REST (Representational State Transfer) was chosen. Within the CST a specification was elaborated. In this specification the existing CORBA interfaces were transitioned into REST. Further optimization to the interfaces is subject of future work.

Access Control

Basic tenet 3, 4 and 6 make authentication and authorization mandatory for a ZTA. As a result of implicit trust, authentication and authorization on a technical level is not required by the standard and is only implemented as an optional vendor-dependent feature (which is extensively done). This vendor-based approach however is a risk to interoperability, as in multinational operations the used approaches have to be coordinated. To enable ZT, all involved assets, resources and processes should be identified and secured with an appropriate security mechanism. Due to the large number of vendor-specific CSD-Servers that can be connected in a multinational environment, it is possible that in the future varying security mechanisms are in use. Therefore, it makes sense to support several variants of access control at the same time. The CST is currently working to introduce and to enforce authentication and authorization in the standard. To gather initial experience how to combine the standard with a security mechanism, HTTP Basic authentication is currently being used as an easy-to-implement variant. In parallel, state-of-the-art security mechanisms, such as authentication keys and certificate-based authentication are considered and evaluated.

Data Integrity

According to basic tenet 5, asserts are not trustworthy and therefore it must be ensured that the asserts have not been manipulated. The correctness, completeness and consistency of the asserts should be guaranteed by data integrity. The current version of the standard does not yet contain any specifications to ensure this. In addition, the internal network was regarded as a secure environment and the assumption was made that there was no threat from within. To make the standard capable of data integrity, a mechanism must be introduced to ensure that all data, i.e. metadata and product file, cannot be manipulated.

A data integrity extension to recognize the corruption of the product file has been developed and used by vendors in recent years and proposed to the CST. As mentioned earlier the extension can be applied by extending the core data model of the standard. For ZT, such an extension should be adopted by every nation and ideally included in the standard. Beyond that, since ZTA requires data integrity for all asserts, the data integrity of the metadata must be established in addition to the data integrity of the product file.

ADAPTIONS IN OUR SYSTEM AND TESTING

As presented in the previous chapter several working fields were identified, namely the replacement of the legacy technology, the introduction of access control and the enforcement of data integrity. To migrate to ZT, these changes must be implemented and tested between multiple nations to guarantee that data exchange is still possible. As we provide the German implementation of the AEDP-17 (namely Fraunhofer IOSB CSD PLUS Server), we have also implemented these changes in our system. In the next subsections we elaborate the necessary adaptions in our system.

Legacy Technology

For the implementation of REST, the intention was that the CORBA interfaces should remain unchanged and the new REST interfaces being offered simultaneously to not break backwards compatibility. The core logic of the system remained the same, with an additional REST adapter only.

After a mature version of the specification for the replacement of CORBA was implemented by the participating nations and the corresponding software components were adapted accordingly, an initial test was carried out at CWIX (Coalition Warrior Interoperability Exercise) 2023. As described in (NATO, 2024), the CWIX is the largest multinational NATO test event in which, among other things, the interoperability of the participating nations and systems is tested. During this test, only minor adjustments and rework were identified, which were collected in order to adapt the specification in the further process. The changes were integrated into the systems in a subsequent iteration and it is planned to test them again at CWIX 2024.

To establish a test event in which each participant must be present is a complex and costly undertaking. Thus, the NSF (NATO Software Factory) was set up to enable a networked test environment to verify even minor changes and keep the test intervals at a minimum. NSF is a cloud environment hosted by the NCIA (NATO Communications and Information Agency), which can be accessed via remote connection once permission has been granted (NCIA, 2019). Software of the participating nations can be deployed within this environment. For risk mitigation for the upcoming CWIX 2024 exercise tests are carried out in this environment for new (security related) features.

Access Control

As it was originally the vendor's decision whether and how to implement access control, our Fraunhofer IOSB CSD-Server already has the option of authentication and authorization via HTTP Basic authentication. For this reason, the adjustments in our implementation to fully adapt HTTP Basic authentication have been only limited to the new REST interfaces (see above). In addition, we have already prototyped authentication keys and certificate-based authentication in our system. To be independent of the other vendor choices, we are currently experimenting with Keycloak as an open source identity and access management solution. By Keycloak's support of several authentication providers, we hope to achieve the greatest possible flexibility.

Data Integrity

At present, we are engaged in the process of analyzing and researching the steps to expand our system in order to ensure data integrity. We want to make sure that the data remains unchanged from the ingest, through the storage in the database, to forwarding to partners, even across security boundaries. To this end, we are currently reviewing the processes involved. Besides the requirements of a ZTA we are also evaluating the requirements of the Federal Office for Information Security (BSI).

In order to support the proposed data integrity extension, adjustments are necessary in our system.

CONCLUSION

Security standards are increasingly coming into focus and become significantly stricter. The shift to ZT is desirable, but migration is not trivial and is rather a marathon than a sprint. Nevertheless, the ambition to move towards a ZTA should be continued. Especially in the case of an interoperability standard the migration involves several steps. Based on the current efforts done in the CST, we considered the associated changes for our system. We have integrated the technology REST into our system to be able to replace the legacy technology CORBA in the future. Additionally, we prototyped and experimented with authentication and authorization mechanism and Keycloak as identity and access management solution.

In our future research, the topics of access control and data integrity will be analyzed in greater depth. For access control, various state-of-the-art mechanisms will be compared. We will check whether we can use our prototype in an operational context. For this purpose, the NSF could serve as a test environment. For data integrity, our first step is to analyze and install the proposed data integrity extension. In a follow-up step, the data integrity of the metadata should also be ensured. This involves considering the applicability of the given extension for metadata. An alternative approach may be necessary.

Further steps to fulfill ZT are an analysis of the processes and systems and the development of a migration plan.

ACKNOWLEDGMENT

Parts of the work of the authors being described in this publication has been funded by the BMVg (Federal Ministry of Defence). The standard STANAG 4559 is developed within the CST of STANAG 4559. The authors acknowledge valuable help and contributions from all partners within the CST.

REFERENCES

Andersen, L. (2017). JEP 320: Remove the Java EE and CORBA Modules. Available at: https://openjdk.org/jeps/320 (Accessed: 10 May 2024).

Computer Security Center (US). (1985). Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (Vol. 85, No. 3). Dod Computer Security Center.

Essendorfer, B., Kuwertz, A., & Sander, J. (2018). Distributed Information Management through Coalition Shared Data. NATO Science and Technology Organization (STO) STO-MP-IST-160.

Henning, M. (2006). The Rise and Fall of CORBA: There'sa lot we can learn from CORBA's mistakes. Queue, 4(5), 28–34.

Kerth, C., Klotz, P., & Essendorfer, B. (2019). A new approach for information dissemination in distributed JISR coalitions. In Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2019 (Vol. 11015, pp. 171–179). SPIE.

NATO. (2024). Coalition Warrior Interoperability Exercise. Available at: https://www.act.nato.int/our-work/exercises/%20coalition-warrior-interoperability-exercise/ (Accessed: 10 May 2024).

NATO Communications and Information Agency (NCIA). (2019). The NCI Agency's Software Factory: a new way to collaborate with industry. Available at: https://www.ncia.nato.int/about-us/newsroom/the-nci-agencye28099s-software-factory-a-new-way-to-collaborate-with-industry.html (Accessed: 10 May 2024).

NATO Standardization Office (NSO) (2018a). STANAG 4559 - NATO STANDARD ISR LIBRARY INTERFACES AND SERVICES. Available at: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8838/ EN (Accessed: 10 May 2024).

NATO Standardization Office (NSO). (2018b). NATO STANDARD ISR LIBRARY INTERFACE-AEDP-17. Available at: https://nso.nato.int/nso/nsdd/main/standards/ap-details/2272/EN (Accessed: 2024 May 10).

NATO Standardization Office (NSO). (2018c). NATO STANDARD ISR STREAMING SERVICES-AEDP-18. Available at: https://nso.nato.int/nso/nsdd/main/standards/ap-details/2273/EN (Accessed: 10 May 2024).

NATO Standardization Office (NSO). (2018d). NATO STANDARD ISR WORKFLOW ARCHITECTURE-AEDP-19. Available at: https://nso.nato.int/nso/nsdd/main/standards/ap-details/2274/EN (Accessed: 10 May 2024).

Stafford, V. A. (2020). Zero trust architecture. NIST special publication, 800, 207.