Enterprise Security Planning with Department of Defense Architecture Framework (DODAF)

L. Ertaul[1], **J. Hao**[2]
[1]Math & Computer Science, CSU East Bay, Hayward, CA, USA
[2]Math & Computer Science, CSU East Bay, Hayward, CA, USA

Abstract – *The U.S Government Department of Defense employs DoDAF to develop and document its large and complex enterprise architecture. DoDAF itself has become a sizable and multifaceted subject matter. This paper is an aggregation of information about DoDAF, serves as a high lever overview and introduction to DoDAF, introducing key terms, concepts and development methodologies, as well as its application in dealing with enterprise security planning related issues.*

Keywords: Enterprise Architecture Frameworks, DoDAF, Enterprise Security Planning

1. Introduction

The Department of Defense Architecture Framework (DoDAF) is an enterprise architecture framework designed to model large and complex enterprises and systems, where their integration and interoperability pose challenges. DoDAF is especially designed to address the six core processes of the Department of Defense (DoD) [1]:

1. Joint Capability Integration and Development System (JCIDS) [1]

JCIDS ensures the capabilities needed for war missions are identified and met. Where gaps between the required and actual capability are identified, appropriate measures must be taken in order prioritize and then bridge those gaps.

2. Defense Acquisition System (DAS) [1]

In order to achieve the National Security Strategy and Support employment and maintenance of the United States Armed Forces, a huge investment has to be made. The DAS is to manage this investment as a whole.

3. System Engineering (SE) [1]

SE looks at family-of-system and system-of systems. Its goal is to balance system performance with total cost while ensuring the developed systems will be the capability requirements.

4. Planning, Programming, Budgeting, and Execution (PPBE) [1]

The PPBE plays an important role from initial capability requirement analysis to decision-making for future programs.

5. Portfolio Management (PfM) [1]

PfM Primarily deals with IT investments. Its goals include maximizing return on investment while reducing associated risks in doing so.

6. Operations [1]

Operations define the activities and their inter-connections that support the military and business operations carried out by DoD.

As explained above, the six processes require decisions to be made at all levels of DoD. The need for an enterprise architecture framework is evident. The next section will outline the history of DoDAF.

2. History of DoDAF

In 1996, the first enterprise architecture framework was developed by DoD. It is called C4ISR. C4ISR stand for Command, Control Communication, Computers, Intelligence, surveillance and reconnaissance. It was developed in accordance to the changing face of modern warfare. [2]

After two iterations of C4ISR, DoDAF V1.0 was release in 2003. It broadened the applicability of architecture tenets and practices to all Mission Areas rather than just the C4ISR community [3]. It addressed usage,

integrated architectures, DoD and Federal policies, value of architectures, architecture measures, DoD decision support processes, development techniques, analytical techniques, (DoD) and moved towards a repository-based approach by placing emphasis on architecture data elements that comprise architecture products [3].

In 2007, DoDAF V1.5 was release. DoDAF V1.5 incorporated net-centric concepts and elements, in order to service and support globally interconnected, end-to-end set of information, capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel [3].

DoDAF V2.0 was published in 2009. In DoDAF V2.0, the major emphasis on architecture development has changed from a product-centric process to a data-centric process designed to provide decision-making data organized as information [4]. The following section will look at this version of DoDAF in more detail.

3. DoDAF V2.0

DoDAF V2.0 consists of 3 volumes:

Volume 1 provides general guidance for development, use, and management of DoD architectures. This volume is designed to help non-technical users understand the role of architecture in support of major decision support processes. Volume 1 provides a 6-step methodology that can be used to develop architectures at all levels of the Department, and a Conceptual Data Model (CDM) for organizing data collected by an architecture effort. [5]

Volume 2 describes the construct of architectures, data descriptions, data exchange requirements, and examples of their use in developing architectural views in technical detail, to include the development and use of service-oriented architecture (SOAs) in support of Net-centric operations. Volume 2 provides a Logical Data Model (LDM), based on the CDM, which describes and defines architectural data; further describes the methods used to populate architectural views, and describes how to use the architectural data in DoDAF-described Models, or in developing Fit-for-Purpose Views that support decision-making. [5]

Volume 3 relates the CDM structure with the LDM relationships and associations, along with business rules described in Volume 2 to introduce a PES, which provides the constructs needed to enable exchange of data among users and COIs. [5]

3.1 Key Terminologies and Concepts

There are several key terminologies used in DoDAF V2.0, which are essential to understanding the framework:
Models: Visualizing architectural data is accomplished through models (e.g., the 'products' described in previous versions of DoDAF). Models (Which can be documents, spreadsheets, dashboards, or other graphical representations) serve as a template for organizing and displaying data in a more easily understood format [6].

Views: When data is collected and presented in a model format, the result is called a view [6].

Viewpoints: Organized collections of views (often representing processes, systems, services, standards, etc.) are referred to as viewpoints [6].

The DoDAF has eight viewpoints as shown in Fig 1. Each viewpoint has a particular purpose. It can be a broad summary information about the whole enterprise, or narrowly focused information for a specialist purpose. It can also be information on the connections and interactions of aspects of an enterprise.

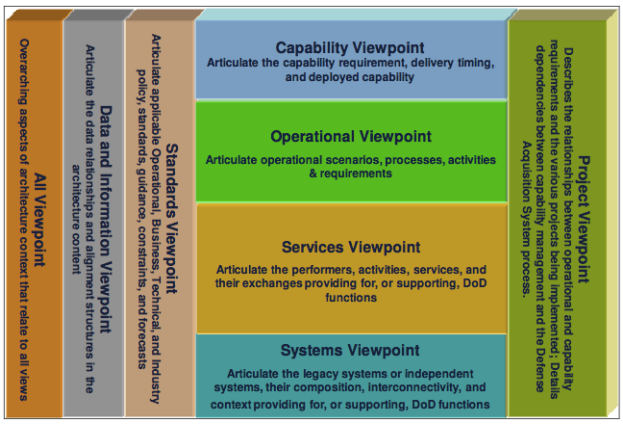

Figure 1. Architecture Viewpoints in DoDAF V2.0

The viewpoints namely are:

All Viewpoint: Some overarching aspects of an Architectural Description relate to all the views. The All Viewpoint (AV) models provide information pertinent to the entire Architectural Description, such as the scope and context of the Architectural Description. The scope

includes the subject area and time frame for the Architectural Description. The setting in which the Architectural Description exists comprises the interrelated conditions that compose the context for the Architectural Description. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations (CONOPS); scenarios; and environmental conditions [8].

The Capability Viewpoint: The Capability Viewpoint (CV) captures the enterprise goals associated with the overall vision for executing a specified course of action, or the ability to achieve a desired effect under specific standards and conditions through combinations of means and ways to perform a set of tasks. It provides a strategic context for the capabilities described in an Architectural Description, and an accompanying high-level scope, more general than the scenario-based scope defined in an operational concept diagram. The models are high- level and describe capabilities using terminology, which is easily understood by decision makers and used for communicating a strategic vision regarding capability evolution [9].

The Data and Information Viewpoint: The Data and Information Viewpoint (DIV) captures the business information requirements and structural business process rules for the Architectural Description. It describes the information that is associated with the information exchanges in the Architectural Description, such as attributes, characteristics, and inter-relationships [10].

The Operational Viewpoint: The Operational Viewpoint (OV) captures the organizations, tasks, or activities performed, and information that must be exchanged between them to accomplish DoD missions. It conveys the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges [11].

The Project Viewpoint: The Project Viewpoint (PV) captures how programs are grouped in organizational terms as a coherent portfolio of acquisition programs. It provides a way of describing the organizational relationships between multiple acquisition programs, each of which are responsible for delivering individual systems or capabilities [12].

The Services Viewpoint: The Services Viewpoint (SvcV) captures system, service, and interconnection functionality providing for, or supporting, operational activities. DoD processes include warfighting, business, intelligence, and infrastructure functions. The SvcV functions and service resources and components may be linked to the architectural data in the OV. These system functions and service resources support the operational activities and facilitate the exchange of information [13].

The Standards Viewpoint: The Standards Viewpoint (StdV) is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. The StdV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks established, and product lines developed. It includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria that can be organized into profile(s) that govern systems and system or service elements in a given Architectural Description [14].

The Systems Viewpoint: Systems Viewpoint (SV) captures the information on supporting automated systems, interconnectivity, and other systems functionality in support of operating activities. Over time, the Department's emphasis on Service Oriented Environment and Cloud Computing may result in the elimination of the Systems Viewpoint [15].

Under the eight viewpoints, there are 53 models in total. They are provided as pre-defined examples that can be used when developing presentations of architectural data [6]. However, DoDAF is designed as "fit-for-purpose", i.e., all the DoDAF-described models only need to be created when they respontd to the stated goals and objectives of the process owner [6].

3.2 DoDAF Meta Model

An aid to defining and collecting data consistent with DoDAF V2.0 is proved by the DoDAF Meta-model (DM2). This meta-model (a model about data), replaces the Core Architectural Data Model (CADM), a storage format, referenced in previous versions of DoDAF. DM2 is a replacement for the CADM, but does not provide a physical data model. Instead, a Physical Exchange Specification (PES) is provided as an exchange mechanism, leaving the task of creation of a physical data model to the tool vendors. DM2 provides a high-level view of the data normally collected, organized, and maintained in an architecture effort. It also serves as a roadmap for the reuse of data under the federated approach to architecture development and management.

Reuse of data among communities of interest provides a way for managers at any level or area of the Department to understand what has been done by others, and also what information is already available for use in architecture development and management decision-making efforts. Finally, the DM2 can be used to ensure that naming conventions for needed data are consistent across the architecture by adoption of DM 2 terms and definitions [6].

As shown in Fig 2, DM2 has 3 views[16]:

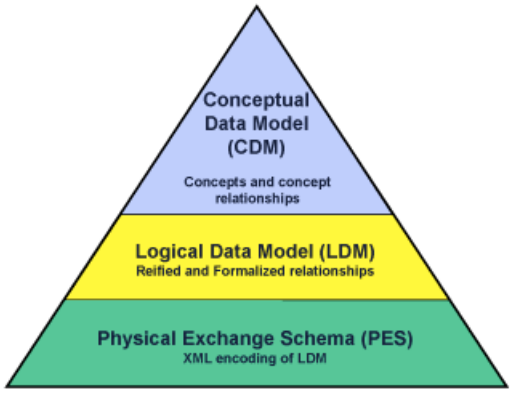

Figure 2. DM2 Views

Conceptual Data Model (CDM) defines the high-level data constructs from which architectures are created, so that executives and managers at all levels can understand the data basis of architecture. The CDM defines concepts and describes their relationships in relatively non-technically and easily understood terms [6].

Logical Data Model (LDM) adds technical information, such as attributes to the CDM and, when necessary, clarifies relationships into an unambiguous usage definition [6].

Physical Exchange Specification (PES) consists of the Logical Data Model with general data types specified and implementation attributes (e.g., source, date) added, and then generated as a set of XSD's, one schema per model/view [6].

In the next section, the DoDAF architecture development methodology is introduced.

4. DoDAF Architecture Development Methodology

DoDAF V2.0 is data-centric rather than product-centric (e.g., it emphasizes focus on data, and relationships among and between data, rather than DoDAF V1.0 or V1.5 products).

DoD employs a 6-step process in architecture development:

1. Determine intended use of architecture: the intended use is generally provided by the process owner. As DoDAF V2.0 uses fit-for-purpose models, the purpose and intended us of the architecture is defined in this initial step [6].

2. Determine scope of architecture: the scope of the architecture is determined by its intended use, as well as its linkage and intersection with other architectures. DoDAF also categorizes the scope of architecture into three levels: department, capability/segment and component level [6].

3. Determine data required to support architecture development: the categories of data needed must first be identified. The levels of details of each data category then need to be determined. Finally, the data that is needed to support architecture development is determined. DM2 provides a set of data definition and categories to aid this this.

4. Collect, organize, correlate, and store architectural data: the data can be collected from existing and/or new processes. In either case, the collected data must be validated and analysed by the subject-matter-experts (SMEs)[6].

5. Conduct analyses in support of architecture objectives: architecture-based analytics is a process that uses architectural data to support decision-making through automated extraction of data from a structured dataset, such as the use of a query into a database [6].

6. Document results in accordance with decision-maker needs: The final step in the architecture development process involves creation of architectural views based on queries of the underlying data. Presenting the architectural data to varied audiences requires transforming the architectural data into meaningful presentations for decision-makers [6].

5. DoDAF and Security

Security is often an add-on after the system is already built. DoDAF, like many other enterprise architecture frameworks, does not address security specifically. The consequence is that the tools and methodologies to perform security related design is not well conceived. Security is sometimes considered as a nonfunctional or performance system requirement, while sometimes a functional system requirement. In some other instances, security is deemed as an operational mission requirement. [17].

To address security requirement concerns, DoDAF identifies the following measure to counter potential threats and to reduce vulnerabilities:

Physical – the counter measures to physical threads, such as break-ins, thefts. Such measures include guards, guard dogs, fences, locks, sensors, including Closed Circuit Television, strong rooms, armor, weapons systems, etc [18].

Procedural – to reduce the risk of exploitation by unauthorized personnel, procedural specification is outlined (e.g. to ensure necessary vetting has been carried out for personnel to access security sensitive information and/or system) [18].

Communication Security (COMSEC) – data in transit is always under the threat of interception. COMSEC addresses such threats by means of encryption and other techniques to ensure the security in data transmission [18].

Transient Electromagnetic Pulse Emanation Standard (TEMPEST) – electronic equipment emit electromagnetic waves purposely or unintentionally. TEMPEST tackles such emission to ensure that no information is disclosed about the equipment, or the data being processed by the equipment [18].

Information Security (INFOSEC) – INFOSEC deals with the basic principles of information security: integrity, integrity, availability and confidentiality of data [18].

The utilization of the above measures reduces the security threat, but it also has adverse effect. The protection mechanisms tend to increase the complexity of the capability fulfillment, and therefore make it difficult and expensive to deploy. DoDAF analyzes the following four characteristics in order to assess the risks and apply minimum but necessary security measures:

Environment - The level of hostility of the environment the asset is exposed to [18].

Asset Value – the cost of the asset to be protected measured by the effect of loss, disclosure and replacement of such asset [18].

Criticality - an assessment of the criticality of the asset to enabling the government to undertake its activities [18].

Personnel Clearance - a measure of the degree of trustworthiness of the personnel that the government deems suitable to access to the asset [18].

DoDAF V2.0 does not have a separate viewpoint for security. Instead, it treats security like any other requirements [17]. DoDAF V2.0 and DM2 are working together to provide the mapping of viewpoints and concepts to the security characteristics. Below is a segment of the mapping table for the service viewpoint.

Table 1. Service Viewpoints and Concept Mapped to Security Characteristics and Protective Measures

Viewpoint	Concept	Security Characteristics	Protective Measures	Notes
Service	Capability Taxonomy	Security Marking Criticality Environment User Security Profile		The security characteristics of a capability taxonomy are to be derived from the constituent services.
	Service	Security Marking Criticality Environment User Security Profile	Physical TEMPEST COMSEC	The environment of a service is derived from the Physical Asset to which is deployed. The User Security Profile is derived from the Organization which uses the service, its Criticality and Security Marking from its Functions.
	Physical Asset	Environment	Physical TEMPEST	The environment identifies the worst environment to which the Physical Asset will be deployed.
	Activity	Security Marking Criticality	INFOSEC Procedural	The Security Marking identifies the maximum security marking of the data the Function will process and the criticality represents the degree of harm to government operations if disrupted.
	Resource Flow	Security Marking	COMSEC	The Security Marking represents the maximum security marking of the Resource Flow.
	Performer and Activity	User Security Profile	Procedural	The User Security Profile is the lowest clearance of the user performing the function. This should be derived from Organizations who perform the Function, if the information exists.

The concepts such as activity, resource flow listed in Table 1 [18] are introduced in DM2. They are the data groups that form the building blocks of the architecture description [19]. Security characteristics are mapped to each of those building blocks to enable the assessment of the security risks and appropriate measures of protection.

6. Conclusions

From C4ISR to DoDAF, the underlying theme of the existence of such enterprise architecture framework to define concepts and models usable in DoD's core processes. DoDAF does so by providing views (models) to represent and document DoD's complex operations, so the broad scope and complexities of an architecture description can be visualized, understood and assimilated. Despite the lack of dedicated security viewpoint, DoDAF is able to deduce the necessary component and concepts needed to implement security requirements.

7. References

[1] http://cio-nii.defense.gov/sites/dodaf20/background.html
[2] C4ISR AWG, C4ISR Architecture Framework Version 2.0, 1997
[3] Department of Defense, DoD Architecture Framework Version 1.5, Volume 1, 2007
[4] http://cio-nii.defense.gov/sites/dodaf20/whats_new.html
[5] Department of Defense, DoD Architecture Framework Version 2.0, Volume 1, 2009
[6] Department of Defense, DoD Architecture Framework Version 2.0, The Essential DoDAF: A User's Guide to Architecture Description Development, 2009
[7] http://cio-nii.defense.gov/sites/dodaf20/viewpoints.html
[8] http://cio-nii.defense.gov/sites/dodaf20/all_view.html
[9] http://cio-nii.defense.gov/sites/dodaf20/capability.html
[10] http://cio-nii.defense.gov/sites/dodaf20/data.html
[11] http://cio-nii.defense.gov/sites/dodaf20/operational.html
[12] http://cio-nii.defense.gov/sites/dodaf20/project.html
[13] http://cio-nii.defense.gov/sites/dodaf20/services.html
[14] http://cio-nii.defense.gov/sites/dodaf20/standards.html
[15] http://cio-nii.defense.gov/sites/dodaf20/systems.html
[16] http://cio-nii.defense.gov/sites/dodaf20/DM2.html
[17] G.C. Dalton, J. Colobi, R. Mills Modeling "Security Architectures for the Enterprise"
[18] http://cionii.defense.gov/sites/dodaf20/security.html
[19] http://cionii.defense.gov/sites/dodaf20/logical.html