Trakia Journal of Sciences, Vol. 8, No. 3, pp 77-82, 2010
Copyright © 2009 Trakia University
Available online at:
http://www.uni-sz.bg

ISSN 1313-7050 (print)
ISSN 1313-3551 (online)

Review

ARCHITECTURE DESIGN OF SECURITY SYSTEM

J. Karakaneva*

New Bulgarian University, Center for Risk Assessment and Security Study, Sofia, Bulgaria

ABSTRACT

The paper is developed according to the DoD Architecture Framework methodology concerning the integration of security requirements in the architecture of the system. This is an overview of the way of the security goals implementation by the incorporation of the security attributes in operational, system and technical architecture models. The risk assessment approach and the means of the architecture environment protection are showed, as well as the inserting of the security attributes into the system architecture.

Key words: DoD Architecture Framework, C4ISR Systems, Security View.

Architecture approach is created in order to define a common unified framework for development, presentation and integration of the systems and it is accepted as strategic concept of defense systems (1).

The main characteristics of the base concept are: interoperability, integration, effective business practices, application of the modern information and communication technology, unified methods of the information systems presentation and implementation.

The methodology gives the rules, guidance and description of the information products for development and presentation of architecture models, providing common base for understanding, comparison and integration of the systems.

The architectures provide the way for comprehension and management of the complex projects. The objective is to improve the ways and means mapping of the requirements and investments, leading to the efficient engineering and the improvement of the operational capabilities for the army and forces management.

Nowadays these systems are transformed into the command and control information systems because the activity of the army and forces management is impossible without precise, timely and reliable information. Regardless of the fact that the methodology is focused on the command and control systems, it is applicable to the human resources management and financing systems, as well defense acquisition.

The approach assures a method for standard description of architecture, and the architecture models present complete consistent information i.e. the final product represents an information model of the system.

The methodology defines three main aspects of the architecture: operational (Operational View - OV), system (System View - SV) and technical (Technical View – TV) and respectively three architecture models (2). In connection with the "sensitive" nature of information in the systems of the security sector arises the necessity of a fourth aspect – security architecture (Security View).

The information security is connected with those attributes, which cover the protection of the operational assets, including information assets. Because security is a critical characteristic, security architecture cannot be considered independently of the rest of the architecture but has to be integrated in it. The security architecture is developed in order to assist the security analyses, the evaluation of the organization's protection against threats

***Correspondence to:** *Assoc. Prof. Dr Juliana Karakaneva; New Bulgarian University, Sofia, Bulgaria; Email:ykarakaneva@nbu.bg*

and the level of application of the security measures to the operational assets necessary to achieve the relevant security level.

The security policies and law are the foundation for the definition of the required security level and the development of the systems. Security engineers are responsible for this area of interest (the components, which need protection), including the measures relevant to the security policy. This area usually has different scope – it can be the whole government or one separate software package. The certification and accreditation of the system is necessary to specify that the security policy is fully applied i. e. the relevant area of interest is completely protected.

The system engineers take into account the security policy during the architecture design. The security engineers plan the implementation of the policy according to the accreditation criteria and the system engineers have to execute the necessary measures and tools of protection. The system and security engineers discuss the project problems and take decisions about the security measures depending on the expenses to achieve the relevant protection.

It is necessary to make analyses of security during each stage of the system engineering process. The security requirements complement the system requirements and both specify the system architecture model and its implementation. The security objectives are identified and risk assessment is accomplished in order to achieve precise understanding of these objectives.

The architects develop the products, containing security attributes, relevant to the security objectives.

The Risk Assessment

The risk assessment provides confirmation that the security measures applied in architecture perform a protective function concerning valuable assets of the system.

The first step is defining the security objectives **(Table 1)**. The procedures engaged for all levels of security depend on the approach in the choice of objectives.

Table 1. *Objectives*

Objective	Definition
Confidentiality	Ensures secrecy
Integrity	Ensures the impossibility to modify or loose information
Availability	Ensures that a system is operational, functional, and accessible at a given moment
Accountability	Ensures that responsibility for a given action or event is inherent to a definite actor through right or obligation

The levels of risk are determined by the assessment of the degree of damages, which can arise and the probability of occurrence of the scenario provoking such damages **(Table 2)**.

Table 2. *Definitions*

Asset assessment	Definition
Scenario	Describes a series of steps or events that occur to produce a damage effect
Level of protection	The amount of resources necessary to prevent this scenario
Damages	Degree of the damages resulting from a scenario
Probability of Occurrence	The probability for this scenario to occur

It is necessary to describe the damage effects, which will occur as a result of a dangerous scenario **(Table 3)** (2).

Table 3. *Damage effects*

Damage effects	Definition
Catastrophic	Death, financial ruin, loss of critical information, operations/system destruction, widespread environmental destruction, failure to determine responsible party for catastrophic effects or modification of an asset that results in catastrophic effects, disclosure of information leading to a catastrophic effect.
Major	Moderate to severe injury/illness, moderate to great financial loss, loss of important to proprietary information, operations/system disruption for an hour or more, moderate to great environmental destruction, failure to determine responsible party for major effects or modification of an asset that results in major effects, disclosure of information leading to a major effect.
Minor	Moderate injury/illness, moderate financial loss, loss of any non-major information, operations/system disruption that lasts for under an hour, failure to determine responsible party for minor effects or modification of an asset that results in minor effects, disclosure of information leading to a minor effect.
Nominal	Light illness, light financial loss, insignificant operations/system disruption.

The next step is the assessment of the probability that the threat, which can provoke damages and losses, will occur **(Table 4)**.

Table 4*. Probability of threat occurrence*

Probability	Definition
Frequent	Possibility of repeated incidents within the short term
Likely	Possibility of isolated incidents within the short term
Occasional	Possibility of repeated incidents within the long term
Remote	Possibility of isolated incidents within the long term
Improbable	Practically impossible

The level of protection **(Table 5)** is a product of damage effect and probability of occurrence.

Table 5. *Level of protection*

Level of protection	Definition
High	Requires to allocate a substantial amount of resources to avert (X > 70% of allocated resources)
Medium	Requires to allocate a moderate amount of resources to avert (20% < X < 70% of allocated resources)
Basic	Requires to allocate a minimal amount of resources to avert (X <= 20% of allocated resources)

Depending on the above defined level of protection the decision makers include the necessary resources in order to minimize the expected damage effects.

All defined notions are connected with the risk assessment for the organization.

The aim is to identify the most valuable assets of the organization and after that to ensure the necessary functionality for the protection of these assets with the corresponding confidentiality, integrity, availability and accountability concerning the system. The decision makers have to define what are the relative probabilities, damage effects and levels of protection. Following these results, the system engineers responsible for the security can plan the required functionality for organization assets protection.

After the risk assessment is completed, it is possible to develop the security architecture as a part of system architecture. The security attributes, which assure the level of protection, are documented in architecture products. The analysts determine whether the architecture corresponds to the defined level of risk.

During this activity the system engineers set the architecture products, including the level of the risk and the necessary tools and methods in order to achieve the protection objectives. The appropriate attributes are built in the architecture products SV and in data dictionary.

The Architecture Environment Protection

The security and the protection of information affect the architecture products. The objective is to formulate a functional strategy implementing the security goals. The development of security model (Security View) is elaborated in parallel with the operational model (Operational View). From security point of view common architecture products (All Views) specify security objectives, strategy and critical factors. OV – products specify main objectives for the organization, types of valuable assets, required protection and assets priorities, according to the security. SV– products specify the security systems and the functionality necessary for the achievement of security goals. The technical architecture (TA) represents the standards connected with the security.

The Security Attributes in AV

The security policy of an organization has to contain the description of the assets with the highest risk. For example, data types requiring protection – classified information, unclassified sensitive information, as well as the information about the threats, environment conditions, geographic areas, which are described in the architecture. The product AV1 (Overview and Summary Information) comprises this kind of information.

The business plans, including the budget and risk assessments for business units, are a very important part of the factors determining the choice and priorities concerning the security resources. The law and other normative acts and the security policy of higher administrative level as well as the agreements with other external organizations are included in this product.

The Integrated Dictionary AV2 consists of all data and definitions concerning the security area.

Operational Architecture

Operational Environment

OV–products, which consist of operational environment, include the representation of the degree of importance of objects and the necessity of protection. The attributes concerning the security are assumed to architecture components and for each object is specified a degree of protection.

The important step in this process is the identification of the necessary ways and means for protection. The responsibilities in the organizational aspect are defined and documented i.e. the main actors in the operational nodes are responsible that their actions are documented. The product consists of information about the measures in the case of breach of security procedures.

Besides, the information exchange, described in OV-products, is attended by the security procedure for protection and by the security measures, depending on the information type exchanged. The security attributes are assumed to activities in operational nodes.

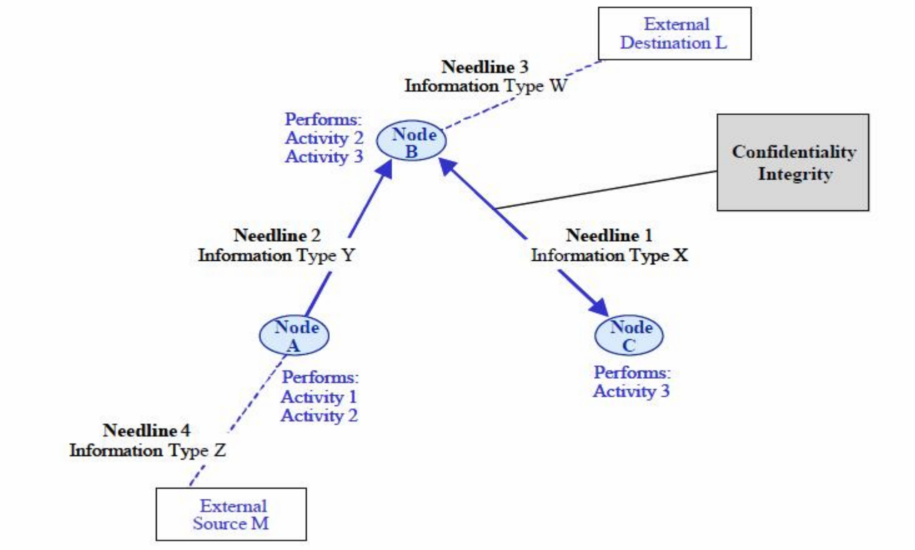

Fig. 1

Fig. 1 following (2) describes the operational nodes and the activities in them. The need lines represent information exchange between the nodes. From security point of view, each exchange of information should be specified by the attributes shown by the protection objective.

For example, the exchange of information between the nodes “B” and “C” has the indicators for confidentiality and integrity. The information above has to be documented in the relevant architecture product (OV5 – Activity Model) with its security attributes.

The Information Objects

The information objects are protected with regard to the main characteristics – confidentiality, integrity, availability and accountability, as well as against non-authorized access and modification of information.

These kinds of attributes are included in OV3 Matrix of Operational Information Exchange and in OV7 Logical Data Model as attributes – indicators.

The operational assets also get the indicators showing how critical they are concerning security and what their priority is in connection with the deployment of the security resources. For example, they are marked with a label – high, medium or low. The approaches to the assurance of information objects are prevention, discovery and answer to possible threats.

The Operational Activities

The operational activities connected with the protected operational assets are identified. The access to them is determined in the form of permitted operations – read, write, modify, create or delete. These assets are represented as the inputs/outputs of OV5 Operational Activity Model, the information elements of OV3 Operational Information Exchange Matrix and the entities of OV7 Logical Data Model. The access type is presented in OV5. In this product and also in the OV4 Organizational Relationships Chart are documented the organizations participating in the operational activity and their responsibilities concerning security, for example in connection with planning, special operations, certification and accreditation of the architecture.

In the product OV6a Operational Rules Model are described the operational rules relevant to the security policy. In the products OV6b Operational State Transition Description and OV6c Operational Event-Trace Description respectively are entered the operational states and operational transitions connected with the operations with the required relevant level of protection. For example, the event “mobilization of new contingent” requires the security indicator and appropriate protection.

The System Architecture

The elements tied to the security in the system architecture products are the following:

1. Setting the physical, procedural and automated systems comprised by the products SV1 Systems Interface Description and SV2 Systems Communications Description in conformity with the requirements of security for OV products.
2. Description of the requirements for certification and accreditation.
3. Determining of the responsibilities of the systems and subsystems.

The documentation for the security in the SV products includes the security attribute of the system functions, systems, subsystems, interfaces and the information exchange. The requirements for OV architecture models are mapped to the SV models, concerning the information, assets, special functions, etc. One of the approaches of the information exchange is the use of protected networks, such as the Virtual Private Network (VPN).

Briefly, VPN implements the functionality for information protection during the exchange between the remote nodes. From security point of view VPN is a proven method (3) for the protection of data in the Internet area. The security engineer has to prove that the use of VPN satisfies the security requirements of the organization. For example, because VPN is used for information exchange between firewalls of nodes “B” and “C”, the requirements of *confidentiality* and *integrity* of the information are implemented.

Confidentiality, in the sense that VPN gives the level of security, so that the data from network “B” cannot easily be modified from the breaker and is protected from accidental access.

Integrity, in the sense that the firewalls, which are used, ensure the implementation of the definite exchange protocol (for example IPSec) and this way provide protection of the information.

The system of information protection is treated as a subsystem, embedded in the system architecture. The security attributes are present in the products SV3 Systems to Systems Matrix and SV5 Operational Activity to Systems Function Traceability Matrix.

The links between the information objects and assets, the security functions and the levels of protection are described in the product SV6 Systems Data Exchange Matrix. In this way the system products SV include the security functions, the characteristics of communication lines, the systems structure, the allocation of the information assets in the systems, as well as the requirements of certification and accreditation of the system and the responsibilities in these processes.

The Technical Architecture

The product TV1 Technical Standards Profile includes the security standards, for example encryption algorithms, protected exchange protocols, etc.

The security components also contain the mechanisms, for example Public Key Infrastructure (PKI), described in special standards. The ways and means are chosen according to the desired level of protection.

CONCLUSIONS

The operational assets, as follows functionalities, organization structures, and data protection is a critical characteristic of the successful fulfilment of all mission and tasks in the security sector. In general the security architecture is a very important component of the architecture model of a system in that area of interest. Through the integration of the security architecture in the architecture model of the system the architects guarantee the accomplishment of the defined security policy. The main steps in this process are the identification of security goals, the risk assessment and the application of methods, procedures and standards for realization of appropriate protection level. The security attributes are embedded in the architecture products during the development of operational, system and technical architecture and they are the special segment of the architecture data model.

Appendix: Architecture Products, according to the DoD Architecture Framework

- AV-1: Overview and Summary Information
- AV-2: Integrated Dictionary
- OV-1: High-Level Operational Concept Graphic
- OV-3: Operational Information Exchange Matrix
- OV-6a: Operational Rules Model
- OV-6b: Operational State Transition Description
- OV-6c: Operational Event-Trace Description
- SV-2: Systems Communications Description
- . SV-3: Systems-Systems Matrix
- SV-5: Operational Activity to Systems Function Traceability Matrix
- SV-6: Systems Data Exchange Matrix
- SV-7: Systems Performance Parameters Matrix
- SV-8: Systems Evolution Description
- . SV-9: Systems Technology Forecast
- SV-10a: Systems Rules Model
- SV-10b: Systems State Transition Description
- . SV-10c: Systems Event-Trace Description
- . TV-1: Technical Standards Profile
- TV-2: Technical Standards Forecast

REFERENCES

1. DoD Architecture Framework Version 2.0, DoD Chief Information Officer (CIO), 2009.
2. DoDAF Deskbook, V. 1.0, 2004.
3. C4ISR Architecture Framework, V. 2.0, Architecture Working Group, Department of Defence, 1997.